How can Privacy Impact Assessments be adapted to the Health Sector in Ireland?

Muireann O'Dea

A dissertation submitted to the University of Dublin,
in partial fulfilment of the requirements for the degree of
Master of Science in Health Informatics

2009

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed: _____

Muireann O'Dea
Date:

Permission to lend and/or copy

I agree that the Trinity College Library may lend
or copy this dissertation upon request.

Signed: _____

Muireann O'Dea
Date:

Acknowledgements

The author acknowledges and wishes to thank the following, without whom this dissertation would not have been possible:

Jane Grimson for her excellent supervision and advice.

Gary Davis for his advice and for permission to use material from the Data Protection Commissioner's website in the PIA Handbook.

Peter Lennon for sharing his time and expertise.

My work colleagues who participated in the PIA.

Niall Watts for reviewing it and making helpful comments.

Tom and Sarah for their support over the past two years.

Summary

Privacy impact assessments (PIAs) are an established approach to assessing the privacy impacts of new initiatives. Many jurisdictions have published handbooks on how to carry out a PIA, and in some jurisdictions they are mandatory for certain kinds of initiative. A PIA looks at the privacy risks of an initiative while it is at the design stage and identifies ways to avoid or mitigate the risks.

Electronic Health Records (EHRs) across distributed systems and organisations are increasingly promoted as a way of improving health care and reducing clinical errors. However EHRs can lead to increased privacy risks.

Objectives: To explore how PIA guidelines could be adapted to the health sector in Ireland, and to evaluate the effectiveness of a PIA.

Methods: A PIA handbook was written based on Irish data protection and freedom of information laws and health information guidelines. The handbook was used to carry out a PIA on a real project. The handbook and PIA were evaluated through a survey of the PIA participants.

Results: The PIA did identify privacy risks that might not otherwise have come to light and it led to the development of privacy design principles for the project. The handbook was found to be useful as an introduction to privacy principles and as a way of guiding the process. Some limitations were found due to restricted stakeholder consultation and the fact that the PIA was initiated by the author rather than the target organisation.

Conclusion: A PIA is an effective approach to protecting privacy that complements other measures such as an information security assessment. It is only effective if it is conducted early on in an initiative when it can affect the outcomes; where there is meaningful engagement between the organisation responsible for the initiative and stakeholder groups; and where the organisation takes ownership of the PIA and reviews it periodically during the life time of the initiative.

Table of Contents

Index of Tables

1 INTRODUCTION

Privacy Impact Assessments (PIAs) are an approach to evaluating the privacy impacts of new systems or initiatives while they are at the design stage. They look at compliance with privacy legislation but also at wider ethical issues. A PIA attempts to identify potential privacy breaches before they occur, and so allow the initiative to be changed or, in some cases, abandoned before there has been a significant investment.

The technique of a PIA emerged in the mid-1990's in Canada and New Zealand and has since gained acceptance in other countries including Australia, Hong Kong, the US, and most recently the UK (Bennett and Raab, 2006). The approach to PIAs varies across different jurisdictions in terms of the level of prescription, the types of initiatives to which they apply and in the details of the approach. In some counties they are mandatory for some types of initiative; in other countries they are not mandatory but are promoted as early warning systems.

Enhancements in information technology have both the potential to intrude on or increase the privacy of individuals. PIAs are a way of evaluating both the threats and the solutions offered by information technology, and as a way of ensuring acceptance of new technology by the public (Clarke, 2008).

The aim of the research project was to develop a PIA handbook geared to the health sector in Ireland and to evaluate it based on its application to a real project. The dissertation is structured as follows:

- **Section 2** gives background information on privacy concepts, health information considerations, the health sector in Ireland and the legislative framework around privacy.
- **Section 3** reviews the guidelines and handbooks for PIAs available in other jurisdictions.
- **Section 4** describes how the author developed a PIA handbook for the health sector in Ireland.
- **Section 5** describes and evaluates a PIA carried out on a real project using this handbook.
- **Section 6** contains conclusions and suggestions for further work.

2 BACKGROUND

2.1 PRIVACY CONCEPTS

Although most people consider privacy to be a basic human right, it can be a difficult concept to define, and it has different meanings in different cultures. Article 12 of the Universal Declaration of Human Rights says:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Privacy has been defined as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations" (Clarke, 2006).

Clarke goes on to describe different aspects of privacy:

- **Bodily privacy:** covering issues such as compulsory immunisation, compulsory sterilisation, and the right to refuse medical treatment
- **Privacy of personal behaviour:** this is concerned with aspects of human behaviour such as political activities, sexual preferences, and religious practices
- **Communications privacy:** the ability of individuals to communicate with one another by phone, email, etc. without monitoring
- **Data privacy:** this is concerned with the capture, use and distribution of personal data, often through electronic media.

Lennon (2005, p.32) gives a different categorisation of privacy, based on a report from a Canadian Task Force in the 1970s:

- **Territorial privacy:** this is based on property or territory, and the right to be left alone in this domain
- **Privacy of the person:** this includes protection from physical harassment, freedom of movement and expression, freedom from physical assault and unwanted search or seizure of the person
- **Privacy in the information context:** this is based on the concept that a person has the right to control all information about themselves, apart from certain defined circumstances,

where social values would require them to communicate certain information about themselves to the authorities.

Liginlal et al. (2009) refers to a study by Smith et al (1996) which identified four areas where people have concerns about how their personal information is used by organisations: collection, secondary use, error and improper access.

Bennett and Raab (2006, p.4) describe what they call the "privacy paradigm". This is the concept that society is made up of autonomous individuals, where there are boundaries between individuals and other individuals, and between individuals and the state. They go on to describe the role that privacy plays in a civil society – promoting freedom of association, allowing secret ballots and political participation without interference, protecting research from political interference and shielding the press which acts as a watchdog. They acknowledge four critiques of the privacy paradigm. Firstly, that it allows people to conceal information about themselves and to mislead others. Secondly, that it supports the split between the private domestic, mostly female, world, and the public masculine world. Thirdly, that the right to privacy does not necessarily support a participative, co-operative society. Finally, while information privacy may lead to fairer and more efficient management of personal data, they believe that it cannot halt the rise of surveillance.

Both Clarke (2006) and Bennett and Raab (2006) stress that privacy must be balanced against other competing interests. Clarke quotes Maslow's hierarchy of needs to support the view that in some situations there are more important needs than privacy, such as food, shelter, etc. Bennett and Raab discuss some of the difficulties of finding a balance between privacy and other interests: how can one determine that an appropriate balance has been struck, and who is to make the decision, the public, a government body such as the office of the privacy commissioner or the organisation introducing the initiative? In addition people may be willing to relinquish some privacy for financial or other rewards (Liginlal et al., 2009). Lennon (2005, p.36) quotes a High Court Judge in the summing up for a court case on illegal tapping of journalists:

"…the right of privacy… is not an unqualified right. Its exercise may be restricted by the constitutional rights of others, by the requirements of the common good and it is subject to the requirements of public order and morality".

Most of the PIA handbooks concentrate on data privacy and communications privacy, which are sometimes known as information privacy (Office of the Victorian Privacy Commissioner, 2004, Ontario Information and Privacy Office, 2001, Australia Office of the Privacy Commissioner, 2006). This is not surprising, since the focus of privacy commissioners and most of the legislation to date has

primarily been on data protection. However, the most recently published handbooks recommend the inclusion of other aspects of privacy such as surveillance and the capture of biometrics and body tissue (Office of the Victorian Privacy Commissioner, 2009b, UK Information Commissioner's Office, 2009).

2.2 Privacy Breaches

Privacy breaches can be accidental or malicious and originate either internally or externally. Liginlal et al. (2009) identify human error as a significant cause of privacy breaches. They reviewed 1046 privacy breach incidents and found 67% were caused by human error and 33% by malicious attacks. They defined two categories of human error: a "slip" meaning the "incorrect execution of a correct action sequence" and a "mistake" meaning the "correct execution of an incorrect action sequence".

2.2.1 Internal Accidental

Internal accidental privacy breaches occur when someone with legitimate access to personal data accidentally discloses it. This can occur through lack of awareness of privacy issues, or through mistakes.

One of the most common types of accident is the loss of a laptop. A report by the Ponemon Institute found that almost 4,000 laptops go missing at European Airports every week (Ponemon Institute, 2009). There have been some high profile cases in Ireland including the loss of a laptop from the Department of Social and Family Affairs containing personal and bank details for over 100,000 claimants (Data Protection Commissioner, 2008) and a laptop stolen from Bord Gáis containing bank details of 75,000 customers (The Irish Times, 2009).

2.2.2 Internal Malicious

Internal malicious privacy breaches occur when someone internal to an organisation accesses and discloses personal data for reasons unconnected with its original collection. This is often financially motivated, as in the case of the singer Britney Spears, whose medical details were accessed by at least 19 hospital employees (Security Magazine, 2008).

2.2.3 External Malicious

Privacy breaches may also occur when someone external to an organisation accesses data inappropriately. A report in Security Magazine found that "One in three major UK companies suffered hack attacks on their websites last year"(Security Magazine, 2003).

Medical identity theft is an increasing problem, particularly in countries where access to medical care is expensive. Medical identity theft involves assuming the identity of another person in order to get medical treatment or to make a medical insurance claim. Not only does this have financial

implications for the individual whose identity is stolen, it also adds erroneous entries to their medical record which could compromise their future medical treatment (World Privacy Forum, 2006).

2.2.4 *Cost of Privacy Breaches*

The costs associated with privacy breaches include the cost of lost equipment, loss of customers, costs associated with informing customers and decreased investor confidence. Liginlal et al. (2009) quotes a report from the Ponemon Institute that estimated the cost of a privacy breach at $197 per compromised record in 2007.

In the US publicly-traded companies are obliged to report privacy breaches so the cost of these can be assessed through the impact on the share price, which reflects a loss of confidence in a company's future prospects. Estimates of loss of market value vary from 0.72% to 5.4% (Liginlal et al., 2009).

2.2.5 *Privacy Breaches in Ireland*

There is no obligation on public or private bodies in Ireland to report privacy breaches, so we can assume that these are underreported. Following recent publicity about lost laptops there have been calls for mandatory reporting of privacy breaches (T J Macintyre, 2009). However others including the UK information commissioner have argued that this can lead to the public ignoring notifications because of "privacy breach fatigue" (UK Information Commissioner's Office, 2008b).

Where individuals find out about privacy breaches they may report it to the Office of the Data Protection Commissioner. There were 1031 complaints in 2008 (Office of the Data Protection Commissioner, 2009).

In his 2008 report the Data Protection Commissioner noted that:

"A collapse of public trust in data-dependent services organisations would be hugely damaging. It would carry a hefty economic price-tag as we would be less competitive and less attractive as a market. The social consequences would arguably be worse. Our public administration would be hopelessly hamstrung. More people would fall through the gaps in our social services and fewer people would receive assistance when they need it."

2.3 HEALTH INFORMATION RELATED ISSUES

Health data is considered by most people to be particularly sensitive and it is categorised as "sensitive data" in the Data Protection Act. In a survey by the Office of the Data Protection Commissioner (2008) 84% of people thought that "privacy" was very important, and ranked privacy of their medical records as the top priority, above categories such as financial history, social welfare history and personal emails (Office of the Data Protection Commissioner, 2008b). The following sections discuss some of the challenges in safeguarding the privacy of health information.

2.3.1 ELECTRONIC HEALTH RECORDS

Privacy issues and concerns apply both to manual and electronic health records. However electronic health records magnify some of the risks but also have the potential to provide greater privacy. Carter (2000) describes a New Zealand Health Intranet Privacy Impact Assessment which warned that "any identifiable information in electronic form is capable of being used, indexed, linked, profiled and compiled in ways which have not been possible with paper records".

A lifelong virtual Electronic Health Record (lvEHR) is seen as a prerequisite to the delivery of the best quality health care (van der Linden et al., 2008). An lvEHR is typically spread across multiple heterogeneous systems and organisations. This leads to a number of security and privacy issues:

- **Authorised access** – how is system access controlled across multiple systems and organisational boundaries
- **Confidentiality** – if data is copied from one system to another how can we be sure that a breach of confidentiality has not occurred on the second system
- **Patient consent** – should patient consent to capture and exchange their data be explicit or implicit, and how can the level of consent be managed across disparate systems
- **Ownership of information** – if copies of the data reside on multiple systems who is the owner of the data, and who is responsible for ensuring that all copies of the data are up to date (van der Linden et al., 2008).

Van der Linden et al (2008) identify the following privacy and security requirements for an effective lvEHR:

- Security – including authentication, authorisation, data integrity, non-repudiation, confidentiality
- Consent – obtaining, recording and tracking of patient consent to capture and use data for specific purposes over specific time-frames
- Semantic interoperability – the ability to share data between systems and automatically interpret it correctly in each system
- Author responsibility – the tracking of the author of each data record
- Audit trail – a record of who, when and what changes were made to a record
- Version control – the ability to have multiple versions of a data item, to know which version was used, and to propagate changes to a data item appropriately
- Patient access – the facility for patients to access their own data
- Archiving and data retention – the ability to store data for the legally required period, and to prevent deletion during this period, and the ability to archive and restore data to off-line storage without loss of information

2.3.2 CONSENT

In order for the processing of health information to be considered fair the patient should consent to its collection, use and disclosure to other parties. Consent requires that the person is aware of and has the capacity to understand the data to be captured and the proposed uses of this data, and that they are aware of options to limit this consent, and are not subject to any coercion (Lennon, 2005, p.137-8).

Consent can be managed through an opt-in or opt-out approach and can be explicit or implicit. The capture of explicit consent can pose problems in a healthcare environment, as it may be time consuming and interfere with the health care. An opt-out approach is simpler to administer and leads to greater inclusion. However an opt-in approach is regarded as the only guarantee of patient privacy (van der Linden et al., 2008).

2.3.3 *CONFIDENTIALITY*

Confidentiality is the duty to ensure that data is only accessed by those authorised to access it. Confidentiality is part of the ethical principles for many professions, including law, medicine, journalism and psychology. The duty of confidentiality is embodied in the Hippocratic Oath:

> "All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."(Wikipedia, 2009)

It is also reflected in the Irish Medical Council *Ethical Guide*:

> "Confidentiality is a time-honoured principle of medical ethics. It extends after death and is fundamental to the doctor/patient relationship." (Irish Medical Council, 2004)

Similarly it is reflected in the Irish Nursing Board *Code of Professional Conduct for Each Nurse and Midwife*:

> "Information regarding a patient's history, treatment and state of health is privileged and confidential. It is accepted nursing practice that nursing care is communicated and recorded as part of the patient's care and treatment. Professional judgement and responsibility should be exercised in the sharing of such information with professional colleagues." (An Bord Altranas, 2000)

The duty of confidentiality is not absolute and there are other rights and duties that must be taken into account, such as where the welfare of the person or another person is at risk, or where there is a legal case. In the public consultation on the forthcoming Health Information Bill the importance of confidentiality of health data was stressed (Department of Health and Children, 2008c).

2.3.4 *LIFELONG NATURE*

A person's health record is by definition lifelong. The lifespan of an IT system could be up to twenty years, so a lifelong EHR will outlive the typical IT system. When an IT system is replaced it is usual for some or all of the data from the old system is transformed and migrated to the new system. With any data migration there is the risk of loss of data integrity, or the loss of metadata, e.g. related to the ownership of the data. The lifelong nature of health information highlights the need for standards and information models that are independent of particular IT system implementations.

2.3.5 *DATA INTEGRITY*

The environment in which health data is captured can pose challenges to ensuring the integrity of the data. For example a busy Accident & Emergency department where PCs are shared across a number of users may lead to data errors.

Where data is copied from one system to another, e.g. where a patient is transferred from one health care provider to another the ownership of the data may be unclear. If the data is subsequently corrected on the originating system the corrections may not be propagated to the other system.

Health Identifiers for both patients and health care providers are seen as important for ensuring the integrity of health data (Department of Health and Children, 2008c). When used effectively they can ensure that health data is linked to the correct person, and that ownership of the data is correctly tracked across systems and health care organisations.

2.3.6 *FAMILY HISTORY*

The taking of a family history is a standard part of a medical consultation, particularly in relation to genetic disorders, paediatrics and psychiatric conditions. Indeed a failure to take a family history could "be used as evidence in negligence or professional standards cases " (Lennon, 2005, p.162). This means that the medical record of one person could include identifiable information about another family member. In some situation it may be an option for the health professional to listen to the family history but not to record the details or at least not to record then in an electronic or easily accessible form.

This issue has been considered in both the UK and Australia and in both cases it was concluded that in some circumstances consent should be sought from family members to the collection of their data, and that they should be informed of the collection (Lennon, 2005, p.162).

2.3.7 *SECONDARY PURPOSES OF HEALTH INFORMATION*

Health information has many secondary purposes other than the primary purpose of providing health care to an individual. Carter (2000) describes some of the potential secondary uses of health information and the agencies involved:

- Pharmaceutical companies may wish to target certain patients to promote new drugs and may be willing to pay for the patient data
- Insurance companies may wish to validate claims

- The data may be required to capture financial data for managing the health service
- Researchers in hospitals, universities and pharmaceutical companies may want access to the data.

Some of these uses of personal health information have economic value which could encourage unauthorised access to the data.

Research using health information often requires data from large populations. This raises the issue of whether a patient has given consent for their health data to be used in this way, and whether or not explicit consent is required. One way of dealing with this is to de-identify the data, but this means that the patients themselves may not be able to benefit directly from the research results.

2.4 IRISH HEALTH SECTOR

The ownership of the Irish health sector is a complex mixture of public and for-profit and not-for-profit private bodies. Approximately 80% of the funding is paid for by the State, and the other 20% is paid directly by patients or through private health insurance (Organisation for Economic Co-Operation and Development, 2005). Many of the large public hospitals such as St James Hospital and the Adelaide and Meath Hospital are owned by private trusts. Within these hospitals consultants carry out work for both public and private patients. A consultant doing private work in a public hospital is regarded as a separate data controller though the patient health data will be held on the hospitals systems. In 2008 the Health Service Executive (HSE) announced "co-location" plans to build private hospitals on public hospital grounds (HSE, 2009). General practitioners, though they receive funding from the State for public patients, are self-employed. All of this leads to complexity in terms of the ownership of data, access to data and the transfer of data between health care providers and organisations.

The "information society" is a term used to refer to the ubiquitous use of information technology in all aspects of life. Over the past 20 years Ireland has embrace the information society. Statistics from the Central Statistics Office show that by 2008, 96% of enterprises with 10 or more employees had computers with Internet access, and 83% had broadband access. For householder the figures are 70% with a computer and of these 89% have an Internet connection, with 31% having a broadband connection. Despite this a 2004 report from the Information Society Commission showed that investment in ICT in the health sector had lagged behind investment levels internationally and investment levels in other sectors (Information Society Commission, 2004). The Brennan Commission report in 2003 noted "under development of information systems throughout all aspects of the Irish health service from policymaking through to implementation" (Brennan Commission, 2003).

However the HSE transformation programme 2007-2010 states the following:

"Central to this programme is the development of a unified national ICT infrastructure and support services and the development of clinical and administrative systems. This will involve establishing national ICT governance structures, integration with shared services, ICT staff development and engagement with health professionals to drive ICT based transformation."(HSE, 2006)

Though the speed of transformation is uncertain it is clear that the next few years will see increasing moves to electronic health records which will challenge the traditional approaches to preserving privacy and confidentiality of health information.

2.5 LEGISLATIVE FRAMEWORK

The privacy of individuals in Ireland is governed by a wide range of legislation including the Constitution, the Data Protection Acts and the Freedom of Information Acts. These "create a patchwork of privacy rights and responsibilities" (Lennon, 2005, p.34).

The Irish Constitution includes an implicit right to personal privacy under article 40.3.1 which states: "The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens". The *personal rights* have been interpreted by the courts as including the right to privacy.

Irish Common law, which is derived from case law rather that the Constitution or statute law, provides some privacy protection in areas such as trespass, defamation, negligence and confidence. However since most of this law predates the modern Information Age, it was primarily "constructed to protect privacy in the context of property and in the enjoyment of property" (Lennon, 2005, p.38).

The main legislation governing data protection and privacy in Ireland are the Data Protection Acts, 1988 and 2003. The Data Protection Act 1988 was based on the 1981 Council of Europe *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*, which came into force in October 1985. The Data Protection (Amendment) Act 2003 incorporated the provisions of EU Directive 95/46/EC *Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data* into the Irish legislation.

The introduction of data protection legislation in Ireland was largely driven by economic factors to do with establishing minimum standards for data protection to allow for the free movement of data between states with equivalent standards. The 1988 Act facilitated the introduction the International Financial Services Centre in Dublin, while the 2003 Act was linked to the setting up of the Internal Market within the EU (Lennon, 2005, p.48).

The Data Protection Acts includes the following definitions:

- A **Data Controller** is "a person who, either alone or with others, controls the contents and use of personal data".
- A **Data Subject** is "an individual who is the subject of personal data"
- **Personal Data** is "data relating to a living 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"

- A further category of data which required special protection is called **Sensitive Personal Data** and this includes, among others, data related to the physical or mental health or sexual life of the individual.

The legislation obliges Data Controllers to:

1. Obtain and process information fairly and with the consent of the individuals concerned
2. Collect and process personal data for explicit and lawful purposes
3. Not use or disclose personal information for purposes other than those identified, except with the explicit consent of the individual
4. Protect the data with appropriate security measures
5. Keep it accurate, complete and up-to-date
6. Limit the data captured to that which is required for the identified purposes
7. Retain it only as long as necessary for the identified purposes
8. Provide an individual with a copy of their personal data, on request

These obligations are consistent with the "fair information principles" which appear in data protection and privacy legislation throughout the world (Bennett and Raab, 2006, p.12).

The Data Protection (Access Modification) (Health) Regulations, 1989 permits a data controller to refuse to provide an individual with a copy of their personal health data where this is likely to damage their physical or mental health (Government of Ireland, 1989).

Part 4 of the Disability Act 2005 contains rules concerning genetic testing, i.e. the testing of a person's DNA/RNA to identify existing diseases or a pre-disposition to particular diseases. The act prohibits the use of genetic testing in relation to insurance policies, health insurance, pensions and mortgages, and requires the prior approval of the Data Protection Commissioner in relation to employment (Government of Ireland, 2005a).

Telecommunications, including phone, e-mail, SMS and Internet use, are governed by the ePrivacy Regulations 2003 which gives effect to the EU ePrivacy Directive 2002/58/EC (Government of Ireland, 2003a). The objective of the directive is to "ensure that consumers and users receive the same level of protection of personal data and privacy, regardless of the technology by which a particular service is used" (Lennon, 2005, p.50). Under these regulations service providers are obliged to

- Ensure the security of their systems and networks
- Ensure the confidentiality of the data
- Erase traffic data when it is no longer needed

And individuals have the following rights:

- To not be identified using calling line identification
- To give consent to the use of location data, i.e. data that identifies the geographic location of a device
- To be informed if they are to be included in a directory, and have the right to opt-out.

These regulations were amended by SI 526 of 2008, to include further restrictions on direct marketing and unsolicited communications. An earlier Act, the Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993, regulates wiretapping and electronic surveillance.

The Freedom of Information (FOI) Acts, 1997 and 2003 place obligations on central and local government bodies and other public bodies in terms of transparency and openness. The aim of the acts is to provide greater transparency into how public bodies operate and make decisions. It confers the following rights on individuals:

- To know what personal data is held about them
- To have inaccurate personal data corrected
- To know the reasons why a decision relating to them was made.

In the case of a minor these rights can be exercised by their parent or guardian and in the case of a deceased person by the next-of-kin or personal representative of the deceased (Government of Ireland, 1997a, Government of Ireland, 2003b).

There is an overlap between the rights conferred by the FOI Acts and those conferred by the Data Protection Acts. Indeed the Data Protection Act includes a clause to say that the any right conferred by the Data Protection Act does not prejudice a right conferred by FOI and that the two commissioners should co-operate. The provisions of the Data Protection Acts apply to living people only, whereas FOI applies to living and deceased persons.

The Health (Provision of Information) Act, 1997, was enacted to facilitate cancer research and screening. It permits any person to provide any personal information to the National Cancer Registry Board for the purpose of any of its functions; or to public bodies for the purpose of cancer screening programmes (Government of Ireland, 1997b).

Under the Medical Practices Act 1978, the Irish Medical Council (IMC) has the authority to regulate the ethical behaviour of doctors. The IMC Ethical Guide includes guidelines on confidentiality, consent, and research, such as:

- "All medical records in whatever format and wherever kept, must be safeguarded".
- "Informed, written consent must be obtained if patients are to be involved in clinical trials or any form of research".
- "Refusal to participate in research must not influence the care of a patient in any way".

The Social Welfare Consolidation Act 2005, paragraph 265, allows for the sharing of information between the Department of Social and Family Affairs and other public bodies for specific purposes, such as the provision of medical benefits for certain members of the public (Government of Ireland, 2005b).

2.5.1 HEALTH INFORMATION BILL

The Department of Health and Children is in the process of drafting a Health Information Bill, following a pubic consultation phase in 2008. A discussion paper on the Health Information Bill states that the objective is to "ensure that there is a sound legislative base for the use and sharing of information throughout the health system so as to provide best patient care and safety and make certain that health information can flow between the public and private health sectors in line with patient care requirements"(Department of Health and Children, 2008b). The discussion paper stresses the importance of protecting the privacy, confidentiality, security and integrity of health data, while at the same time balancing the rights of individuals against the needs of those providing health care and doing research.

Many jurisdictions, including the US, some Canadian and Australian states and New Zealand have legislation governing health information which aims to promote better use of health information through measures such as

- Standardisation of the format of health information to facilitate exchange of data
- Prescribing the format of health identifiers for patients and health providers

- Defining standards to protect the privacy and integrity of health information
- Rules on the use of health information for research
- Rules on the setting up of national population registries, e.g. cancer registries.

Medical research is important for both individuals and the population as a whole. Some types of medical research require identifiable personal information, which means that under the Data Protection Act, explicit consent would be required for this use. In the UK the Health & Social Care Act 2001 gives the Secretary of State for Health the right to bypass matters of consent for management and research purposes, where it is not practicable to obtain consent. In Canada the Federal Personal Information Protection and Electronic Documents Act permits organisations to get exemption for obtaining consent for the use of information for scholarly research (Lennon, 2005, p.230-233).

National population registries provide a repository of information for research and planning. For them to be useful it is important that they include 100% of cases, that there is no duplication of cases and that it is possible to identify major events, such as the death of a patient. The setting up of new registries can be hampered by the need for consent, particularly where they are based on existing data. This has been handled on an ad-hoc basis in Ireland through legislation such as the Health (Provision of Information) Act 1997 which facilitated the setting up of the National Cancer Registry. Canada has an extensive array of population registers, but access to these is limited to a small number of analysts and there are strict controls over the data that is published to avoid re-identification of patients. In the UK the Health and Social Care Act 2001 allows the Secretary of State at the Department of Health to permit use of health data without explicit patient consent. This has been used to allow the setting up of cancer and other registries.

Unique health identifiers for patients and individual health care providers are seen as a prerequisite for the building of electronic patient health records. They allow linking of all data related to a patient regardless of where it was captured, and facilitates sharing of data across organisations, which results in better patient care and less duplication of medical tests.

Some countries, such as Finland, use the social security number as the health identifier. In Ireland the Personal Public Services Number (PPSN) was originally introduced as an identifier for public services including social welfare, revenue and healthcare. However, it has not been used widely as an identifier for healthcare. The Health Information Strategy reviewed various approaches and recommended the use of the PPSN. However, in a submission on the proposed Health Information Bill, the Data Protection Commissioner rejected the use of the PSPN as a Unique Health Identifier, as

it “would open up people to potential huge invasions of their privacy”(Office of the Data Protection Commissioner, 2008c).

The author met with Peter Lennon, the official within the Department of Health with responsibility for the Health Information Bill. From these discussions it is understood that the bill is due for publication in late 2009 and that it will address the following areas (Lennon, 2009):

- To restate and clarify the rules in relation to personal health information found in the Data Protection and Freedom of Information Acts.
- To establish a basis for population health registers. Up to now these have been handled on a once-off basis. The Health Information Bill will establish a framework for population health registers in general, including considerations such as mandatory reporting.
- To specify what will be used as the national health identifier, i.e. whether it will be based on the PPSN or whether a new identifier will be established.
- To establish a national medical ethics body. As of April 2009 there are 57 medical ethics committees in Ireland, which can pose a significant challenge to researchers who are doing research on a national basis, since they may need to get approval from all 57 ethics committees which can cause delays.
- To require a privacy impact assessment for some types of initiatives. The details of the privacy impact assessment are likely to be contained in regulations after the bill. The results of the privacy impact assessment will be required to be made public. A formal approval process of the privacy impact assessment will not be required, as it is felt that this could cause delays to new initiatives.
- To improve the controls around genetic testing, which are covered in the Disability Act 2005.

2.6 TECHNOLOGY

Concerns about the privacy of health information pre-date recent developments in information technology, however these developments have brought these concerns into sharper focus. Bennett and Raab (2006) assert that data protection and privacy legislation have been designed "in large measure, to control the worst effects of technologies". Technology has both the potential to intrude on or enhance privacy. These technologies are sometimes called PITs (Privacy Intrusive Technologies) and PETs (Privacy Enhancing Technologies). Both categories of technology should be considered when assessing the privacy impacts of a new initiative.

2.6.1 PRIVACY INTRUSIVE TECHNOLOGIES

Cookies are a widely used PIT. They are files that are downloaded onto a PC when a user visits a website. They allow the website to track information about the user, such as passwords, and to remember this information between sessions. This can be useful to the user, however they also allow the website to build up a profile of the user, and they also leave a record of the sites visited on the user's PC. Most Web browsers now allow users to block cookies or to only allow them from some sites, or to have single-session only cookies (Alban et al., 2005).

A second example is "spyware" which is a computer program that is installed on a personal computer without the users consent. The spyware may monitor their browsing habits, install other programs, redirect the browser, or display advertising material. Some spyware can slow down the performance of the PC (Forte, 2005).

A third example is the tracking of telephone calls. Telephone billing systems track the calling and called number for all telephone calls, and for calls from mobile phones, the location of the cell from where the call was made. This has been described as "surveillance by design" (Bennett and Raab, 2006, p.183).

While users can guard against cookies and spyware without any major loss of functionality, it is more difficult to control the monitoring of telephone calls without restricting one's ability to communicate with others.

2.6.2 PRIVACY ENHANCING TECHNOLOGIES

Bennett and Raab (2006, p.181) identify three categories of PET: the first category is "systemic instruments" arising from design decisions of the hardware and software engineers who design and build the systems; the second category is "collective instruments" which are a result of government policy; and the third category is "instruments of individual empowerment" which give individuals options to select enhanced privacy in their transactions with an organisation.

As an example of the first category they describe the network design for two Universities in the US. At the University of Chicago it is possible for students and staff to connect any PC to the network, thus allowing them to communication anonymously. At Harvard, however, the PC must be pre-registered, so it is possible to identify the source of all interactions on the network. The former is an example of a "zero collection of personal information" approach. If personal information is not captured then there are no issues to do with collection, use and security of the data.

An example of the second category is the development of public-key infrastructures (PKI) for the delivery of public and private services. PKI uses asymmetric keys for encryption and decryption of messages. A user's identity and public key are registered with a certificate authority, who issues the user with a certificate that can be used to encrypt messages. The REACH public services broker in Ireland was an attempt to provide a wide range of public services using a central authentication service based on PKI technology (Department of the Taoiseach, 2008).

The third category includes tools that users can choose to use to enhance their privacy. These include encryption tools, anonymity tools which shield a user's identity, and filters which attempt to block cookies and spyware. The Electronic Privacy Information Center website (www.epic.org) provides an extensive list of such tools.

Bennett and Raab (2006) describe a further group of tools called privacy management instruments, which "attempt to negotiate a consumer's privacy preferences with a website". These allow a website to encode its privacy policy in a machine readable format, a user to record their privacy preferences, and the privacy management instrument to negotiate between the two. Examples of these instruments include the Platform for Privacy Preferences (P3P) which was developed by the World Wide Web Consortium (World Wide Web Consortium, 2007). P3P is a protocol that allows website to declare how they will use information collected from browsing users. The P3P technology has been partially incorporated into Microsoft's Internet Explorer 6.0 so that users can view P3P policies and use this to decide whether to download cookies from a website. P3P is not restricted to use in websites. Agrawal and Johnson (2007) describe how P3P could be used to capture organisational policies, data protection laws and patient privacy preferences in a health information system to allow fine-grained control over access to patient health information.

Another approach to using personal health data for research without patient consent is to anonymise the data. The simplest approach is to remove the identifying data fields. However, a de-identified data set may still be prone to linkage, depending on the patient population involved, e.g. a person of age 80 of Chinese origin living is a sparsely populated area Ireland could easily be identified. A more

sophisticated approach is *k*-anonymisation. This removes some identifying information and generalises some others so that every record is indistinguishable from *k-1* other records (Agrawal and Johnson, 2007).

3 STATE OF THE ART

3.1 HISTORY OF PIAS AND PIA HANDBOOKS

It is difficult to identify the precise origin of PIAs. Clarke (2008) identifies two possible pre-cursors of the PIA: the "technology assessment" and the "environmental impact statement" (EIS). The EIS evolved into a more process-oriented "environmental impact assessment". Clarke notes that the International Association for Impact Assessments, while it has expanded the applicability of impact assessments to a wide range of domains, including social and health, has not yet identified privacy as a sub-domain (IAIA, 2009). All of the researchers agree that the first published use of the term "privacy impact assessment" occurred in the mid-1990s. In 1994 the Ontario Information and Privacy Commissioner, Tom Wright, wrote that "the preparation of a privacy impact statement should be required prior to the introduction of any potentially privacy-intrusive technology"(Bennett and Raab, 2006).

Various rationales have been identified for the use of PIAs. Bennett and Raab (2006) view PIAs as a way of avoiding some of the pitfalls of privacy audits, which they describe as "an expensive and time-consuming process, and many data protection authorities do not have the human resources to conduct an audit program on a regular basis". Clarke (2008) sees two other possible rationales for PIAs. The first is as a concession to the public who have become increasingly concerned about the privacy intrusive nature of many new government and private sector initiatives. The second as a rational management approach to risk assessment and a way of ensuring that a new initiative achieves widespread acceptance.

Over the past 15 years the approach to PIAs has matured and developed in various countries:

New Zealand: The Deputy Privacy Commissioner published two papers in 1996, and in 2002 a PIA handbook was published (New Zealand Privacy Commissioner, 2007).

Ontario: In 1998 PIAs became a pre-requisite for cabinet approval of IT projects and in 1999 PIAs became mandatory for public health initiatives (Ontario Information and Privacy Office, 2001).

British Columbia: The Privacy Commissioner from 1993-99, David Flaherty, advocated and applied the PIA approach to many initiatives and in 2002 a PIA became mandatory for "a new enactment, system, project or program" (British Columbia Office of the Chief Information Officer, 2006).

Alberta: The Health Information Act 2002 requires public agencies to carry out a PIA. PIAs are not mandatory for other sectors but guidelines are provided (Alberta, 2006a).

Canada (Federal Level): The Treasury Board published a PIA handbook and an e-learning tool in 2002 (Canada Ministry of Government Services, 2008).

Australia: During the 1990s various guidelines for data matching programs and usage of PKI were produced, and in 2006 a PIA handbook was published (Australia Office of the Privacy Commissioner, 2006). In 2004 the State of **Victoria** published a PIA handbook (Office of the Victorian Privacy Commissioner, 2004). This was revised in May 2009 (Office of the Victorian Privacy Commissioner, 2009b).

Hong Kong: In 2002 the then Privacy Commissioner recommended the use of PIAs for the state identity card project. However no formal PIA handbook or guidelines have been published.

US: The e-Government Act of 2002 requires PIAs to be conducted for new public sector initiatives as a prerequisite for budget approval (US, 2002) .

UK: In 2007 the Information Commissioner's Office commissioned a project to review of international practice in PIAs and to deliver a PIA handbook (UK Information Commissioner's Office, 2007). Following feedback the handbook has been revised to make more accessible and to give clearer instructions on how to carry out a PIA (UK Information Commissioner's Office, 2009).

Finland: The Finnish government is considering the introduction of a PIA type approach (Linden Consulting, 2007).

Ireland: The Office of the Data Protection Commission has published guidelines on the introduction of biometrics in the workplace (Data Protection Commissioner, 2007). There are no plans to introduce PIA guidelines (Davis,G., 2009).

3.2 Comparison of Handbooks

The PIA handbooks that are available vary considerably in length, approach, and how prescriptive they are. This section compares the handbooks under various headings.

The handbooks that are available at the time of writing (June 2009) are:

- Alberta (Alberta, 2001)
- Ontario (Ontario Information and Privacy Office, 2001)
- New Zealand (Office of the New Zealand Privacy Commissioner, 2002)
- Canada (Canada Treasury Board Secretariat, 2002)

- USA (US, 2002)
- British Columbia (British Columbia Office of the Chief Information Officer, 2006)
- Victoria first edition (Office of the Victorian Privacy Commissioner, 2004), and revised edition (Office of the Victorian Privacy Commissioner, 2009b)
- Australia (Australia Office of the Privacy Commissioner, 2006)
- UK first edition (UK Information Commissioner's Office, 2007), and revised edition (UK Information Commissioner's Office, 2009)

The following terms are used in this section:

- **Privacy Office** = the office responsible for information privacy, i.e. the equivalent of the Office of the Data Protection Commissioner in Ireland
- **Handbook** = a privacy impact assessment guide

3.2.1 DEFINITION OF A PIA

The handbooks offer various definitions of a PIA:

British Columbia: "A PIA is a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy."

Victoria: "Privacy Impact Assessment (PIA) has been defined as 'an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated'."

Australia: "A PIA is an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals – it 'tells the story' of the project from a privacy perspective."

Ontario: "A Privacy Impact Assessment (PIA) is a process that helps determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements."

US: A "Privacy Impact Assessment (PIA)- is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in

identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."

New Zealand: "Privacy Impact Assessment (PIA) is a systematic process for evaluating a proposal in terms of its impact upon privacy."

The key features of these definitions are the focus on the process rather than the final report, the broad definition of privacy rather than just legal compliance, and the emphasis on assessing proposed initiatives rather than existing or completed initiatives.

3.2.2 LENGTH

The PIA handbooks currently available vary considerably in length, from 28 pages in the revised Victoria handbook to 96 pages in the Ontario handbook. The length of the handbooks reflects different approaches: either compliance with privacy legislation or looking at broader privacy issues. The Alberta handbook is terse and focused on the completion of an annotated questionnaire. The UK handbook is discursive and while it does contain a data protection compliance checklist, it aims to guide an agency through consideration of broader privacy issues. The original UK handbook was 113 pages long, but the revised version is only 81 pages, reflecting criticism of the lack of accessibility of the original handbook.

While it is generally agreed that PIAs should take a broad look at privacy issues, the length of some of the guides could discourage organisations from undertaking one. Flaherty (2002) regards the length and complexity of some guides as a major criticism of them. The UK handbook attempts to address this issue by splitting the handbook into a guide for full-scale PIAs and one for small-scale PIAs. However the guide for small-scale PIAs is not a standalone document, rather it refers the reader to the guide for full-scale PIAs in several places, saying that "ideas extracted from this document will need to be scaled, in order to be applicable to the particular project".

The first edition of the Victorian handbook was 36 pages long, while the second edition is ever shorter at 28 pages. However the Victorian privacy office has published two supporting documents:

- A 63 page PIA Report Outline (Office of the Victorian Privacy Commissioner, 2009c)
- A 26 page Accompanying Guide to Privacy Impact Assessments (Office of the Victorian Privacy Commissioner, 2009a)

The approach appears to be that the handbook is a short and simple guide that "sells" the concept of a PIA, while the supporting documents provide detailed reference material for organisations undertaking the process.

3.2.3 BENEFITS OF A PIA

Each of the handbooks extols the benefits of doing a PIA. The main benefits mentioned are:

Risk assessment and risk avoidance or mitigation, where the main risks would be bad publicity and loss of public trust which could lead to rejection of an initiative by the public. The UK handbook notes that "Where the success of a project depends on people accepting, adopting and using a new system, process or programme, privacy concerns can be a significant risk factor that can threaten the return on the organisation's investment".

Compliance with legislation related to data protection, freedom of information, health information, and electronic communications. This is the only reason given for doing a PIA in the Alberta handbook, while the New Zealand handbook stresses that "protection of privacy is more than simply avoiding a breach of the law. It can involve striving for something better".

Cost effectiveness through identifying and resolved privacy issues before there is a significant investment. The New Zealand handbook says "it is cheaper to do things at the design phase to meet privacy concerns than attempt to retrofit them afterwards". In some cases a PIA may lead to a project being abandoned because of privacy risks, before there has been any significant investment.

Education and awareness of privacy issues, both within the project team, within the overall agency for future initiatives, and, where the results are published, among the public and similar agencies worldwide.

Improved consultation with stakeholders, which can enhance the legitimacy of the initiative, especially where there are trade-offs between privacy and other benefits. The Canadian guidelines refer to "building trust and confidence with citizens". The US handbook says that PIAs should ensure "that the American pubic has assurances that personal information is protected". The Australian handbook argues that a PIA enables an organisation to "reflect community values" in a project.

Provide documentation to the relevant privacy office as a basis for discussion, to allow the privacy office to offer advice, and to make any investigations by that office easier and more cost effective.

3.2.4 Approach and Structure

This section compares the various approaches suggested in each of the PIA handbooks for how to carry out a PIA, including the suggested activities, and the sequencing and timing of these.

The most common approach recommended is as follows:

1. A threshold assessment to determine if a PIA is required
2. A preliminary analysis to document the project objectives and, at a high-level, any potential privacy risks
3. The PIA itself, including documenting information flows, analysing privacy risks, assessing alternative approaches, and documenting the results
4. A privacy audit to ensure compliance with legislation after the system or initiative has been implemented

The Canadian handbook recommends the following activities:

Stage	**Activities**
Project Initiation	Define • Scope of PIA • PIA Team • Tools to be used
Data Analysis	Define business processes Identify personal information clusters Map detailed data flows of personal information
Privacy Analysis	Complete questionnaires Discuss answers that require further details Describe privacy issues and implications
PIA Report	Write a report that: • Summarises privacy risks • Identifies and discuss options, and make recommendations • Includes other considerations

The UK handbook places greater emphasis on stakeholder consultation and recommends the following phases and activities:

Stage	Activities
Threshold Assessment	• Assess whether PIA is required, and if so whether this should be a full-scale or small-scale PIA
Preliminary Phase	• Develop project outline and terms of reference for PIA • Hold preliminary discussions with stakeholder groups and privacy office • Conduct preliminary privacy analysis
Preparatory Phase	• Develop stakeholder consultation plan • Form a stakeholder consultative group
Consultation and Analysis Phase	• Consult with stakeholders • Identify privacy issues • Consider design options
Documentation Phase	• Document PIA report including privacy and data protection compliance studies
Review and Audit Phase	• Review PIA recommendations to ensure they have been followed through • Document PIA review report

3.2.5 PIA REPORT GUIDELINES

Most of the handbooks include a recommended table of contents for the PIA report. This is useful for organisations carrying out a PIA for the first time and it also ensures that significant areas are not overlooked. The Canadian handbook includes a full chapter on this with an outline for both a preliminary and final PIA report, and instructions for what should be included in each section. In both Ontario and Alberta a questionnaire is supplied and the required output from the PIA is the completed questionnaire together with documents to support the answers given.

The revised Victoria handbook is supplemented by a detailed 63 page report template. The template includes an introductory section for a description of the project, data flows, how data is collected, used and disclosed, and how data security and data quality are handled. The bulk of the template consists of sections for each of the information privacy principles (IPPs) contained in the relevant legislation (the Victoria Information Privacy, Freedom of Information, Health Records and Charter of Human Rights and Responsibilities Acts). For each principle the organisation is expected to include an

assessment of how well the initiative will comply with the principle, to identify both positive and negative privacy impacts of the initiative, and to answer the following three questions:

- "Will the project comply with this IPP?
- Will the project meet community expectations about anonymity?
- What else can be done to minimise risk and maximise protections in relation to *<relevant privacy principle>*"(Office of the Victorian Privacy Commissioner, 2009c)

The final section of the template is a summary of the most significant findings and critical recommendations. The Victoria handbook emphasises that the PIA report should be a standalone document and, if published, can "be used as a springboard for running stakeholder or public consultation".

3.2.6 BREADTH

The PIA guidelines in different jurisdictions vary in terms of the type of initiative for which they are recommended, and in the breadth of the analysis, e.g. some are focussed on IT systems and information privacy, while others look at a broader range of initiatives and a broader definition of privacy; and some focus on legal compliance with privacy and data protection law, while others look at wider ethical issues.

In the US the requirement to do a PIA arises out of the e-Government Act 2002, so the PIA guidelines are entirely focussed on IT systems and information privacy.

The UK guidelines recommend reviewing all types of privacy risk, where appropriate, including bodily privacy, e.g. submission for biometric measurement, and privacy of behaviour, e.g. CCTV surveillance. The criteria for project selection are focussed on IT related projects, or those that include a significant IT component, and in particular relatively new technologies such as radio frequency identification (RFID) tabs, biometrics, digital signatures.

The first edition of the Victoria handbook focussed on information privacy. However, as a consequence of the Victorian *Charter of Human Rights and Responsibilities Act 2006,* the revised handbook and supporting documents have been extended to other types of privacy including bodily privacy.

The guidelines in other jurisdictions, including Canada, Australia, Ontario and New Zealand are focussed primarily on information privacy and projects with a significant IT systems component,

though they do mention that other forms of privacy such as bodily privacy may need to be considered.

It is not surprising that the focus of most of the guidelines is on information privacy and on IT systems. However, in the context of health information, both bodily privacy and privacy of behaviour are significant. Also, increasing concerns about the "surveillance society", especially since 9/11, would suggest a broader review on privacy (Surveillance Studies Network, 2006).

Information security is not covered in detail in any of the handbooks. The UK handbook states that "One small but important part of privacy protection is information security and some aspects of a PIA need to reflect this". The UK handbook then refers the reader to text books and standards on the subject. The revised UK handbook refers the reader to a *Privacy by Design* report (UK Information Commissioner's Office, 2008a) which describes in greater detail how Privacy Enhancing Technologies (PETs) can be used to enhance privacy. This report describes PIAs as complementing information security assessments by taking an individual's perspective into account.

The handbooks from Canada, Ontario and Victoria recommend that technology and systems experts are included in the PIA team. The Ontario handbook regards the PIA report as providing basic documentation for systems analysts and security analysts. The New Zealand handbook recommends consideration of "security safeguards, privacy enhancing technologies" as risk mitigations.

3.2.7 LEGAL BASIS

Whether or not an organisation is required to do a PIA varies by jurisdictions. PIAs are required by legislation in some jurisdictions, prescribed by policy in others, and recommended in other cases. PIAs are legislatively mandated in Canada and the US for some kinds of initiative. The US e-Government Act (2002) requires government agencies to carry out PIAs when they "when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information". Clarke (2008) describes the requirements as "a mere data protection law compliance checklist" and views the US as "a wasteland from the viewpoint of privacy policy".

The federal Government of Canada requires Government institutions (apart from the Bank of Canada) to "develop and maintain Privacy Impact Assessments to evaluate whether program and service delivery initiatives involving the collection, use or disclosure of personal information comply with privacy requirements and to resolve privacy issues that may be of potential public concern". In British Columbia PIAs are legislatively required for government ministries. In Alberta public health organisations are required to "prepare a privacy impact assessment that describes how proposed

administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information".

PIAs are not legally required in any jurisdiction for private organisations. It is not clear why this is the case, since privacy legislation applies equally to public and private sector organisations. This does not mean, however, that PIAs are unknown in private organisations. Examples of private organisations that have carried out PIAs include TELUS, a Canadian telecommunications company and Hewlett Packard (Linden Consulting, 2007).

In jurisdictions where PIAs are not mandatory, the privacy office attempts to persuade organisations to carry out PIAs by pointing out the benefits to the organisation in terms of risk reduction and early identification of issues. In these jurisdictions the privacy office does not have a role in approving PIAs, but may be involved in an advisory capacity.

When the first UK PIA handbook was published in December 2007 PIAs were recommended but not mandatory. However following the loss of two discs containing 25 million child benefit records (BBC News, 2008) it is now policy, though not legislatively mandated, for all Government Departments and Agencies to carry out PIAs for new initiatives involving personal information (UK Cabinet Office, 2008).

3.2.8 Involvement of Privacy Office

The role that the privacy office or government agencies play in reviewing, approving or accepting PIA reports varies across different jurisdictions. Where PIAs are legally required the privacy office has a role in reviewing them, and in the US and Canada a PIA is required for funding approval of some projects.

In the US the PIA report must be *approved* by the CIO or person at an equivalent level in the agency procuring the system, other than the official procuring the system or conducting the PIA. The PIA report must be *submitted* to the Office of Management and Budget prior to funding approval.

In British Columbia organisations are not required to submit PIA reports to the privacy office. The guidelines recommend consulting with privacy experts on specific questions.

In Ontario organisations are not expected to submit PIA reports to the privacy office, however the guidelines state that the privacy office may use the PIA as a starting point for any investigation into privacy breaches.

In Alberta health organisations are required to submit the PIA to the privacy office in advance of implementing the new initiative. However the handbook states that while the privacy office *reviews* and *accepts* PIAs it does not *approve* them, and the responsibility for complying with privacy legislation rests with the organisation.

In Canada organisations are required to submit the PIA to the privacy office at an early stage in the project, to allow for review and advice from that office. In addition, where funding is being sought, details of the PIA must be included in the submission to the Treasury Board (Canada Treasury Board Secretariat, 2002).

The Victoria states that the privacy office " has an advisory role but cannot conduct a PIA for you" (Office of the Victorian Privacy Commissioner, 2009b).

In the UK the handbook recommends that the PIA report is submitted for review to a consultative group, whose composition is decided as part of the PIA planning process. In describing the role of the ICO the handbook says: "the ICO may be available for consultation on particular projects; but it does not participate directly in any PIA process, and is not responsible for the conduct of any PIA."(UK Information Commissioner's Office, 2007).

In New Zealand the guidelines do not make any reference to involvement of the privacy office in the review or approval of PIA reports. However the guidelines do state that reviewing a PIA report in connection with an investigation is more cost effective for the privacy office, than investigating the business practices.

In Australia the guidelines state that the privacy office does not have any official role in reviewing or approving PIAs, however it does offer assistance on any privacy issues that arise during the PIA process.

3.2.9 WHO CONDUCTS THE PIA

There are various opinions on whether a PIA should be carried out by internal members of a project team or by external privacy experts or consultants. Flaherty (2000) recommends that someone from the project team drafts the PIA and keeps it up to date as the project progresses. However, he also recognises that project teams may lack the background knowledge of privacy legislation and risks, and that they may also be under pressure to meet deadlines to deliver the project and this could conflict with the requirement to deliver a PIA.

The Victoria handbook recommends that individuals from within an organisation should carry out the PIA as this promotes ownership of the PIA and builds internal expertise to deal with issues that may

arise in the future. The Victoria handbook recommends that external consultants with specific skills are brought in to assist with certain aspects, where required.

The Ontario handbook gives a useful description of the types of skills that may be required to carry out a PIA:

- Policy Development Skills
- Operational Program and Business Design Skills
- Technology and Systems expertise
- Risk and Compliance Analysis skills
- Procedure and Legal skills
- Access to Information Privacy expertise

3.2.10 When to Conduct PIA

Most of the PIA handbooks reviewed recommend starting the PIA process early in the project lifecycle and reviewed and expanded as the project proceeds. When the project is complete a privacy audit is recommended to ensure compliance with legislation. Flaherty (2000) regards PIA reports as "protean documents that … evolve over time with the continued development of a particular system". Over the lifetime of the system the PIA report can act as a baseline, when any changes that might affect flows of personal information are proposed.

Both the New Zealand and Ontario handbooks recommends that the PIA is started early, but that it is treated as an evolving document and completed during the latter stages of the project. The New Zealand handbook recommends doing a preliminary PIA during the conceptual definition stage of the project; a full PIA during the system definition and functional design phase, which is reviewed during the system development and implementation phases, and finally a privacy compliance audit when the system becomes operational.

The UK handbook recommends starting the PIA at the conceptual or initiation phase of the project, or "if the project is already under way, start today". Starting the PIA early in the project lifecycle means that design changes to mitigate any privacy risks can be incorporated into the project, before there has been significant effort and money expended on other options. The Alberta guidelines on FOI and privacy compliance say "If the PIA is viewed as an obstacle to the initiative being launched, it has been started too late. If decisions about the initiative are not firm, resources have not been

committed and questions about privacy implications cannot be answered, it is too early to start the process" (Alberta Health and Wellness, 2006).

In jurisdictions where PIA are mandatory for some initiatives they are required to be completed before the initiative is implemented, and in some cases are a prerequisite for funding. In the US, where a PIA is a legal requirement for some projects, the agencies are required to conduct the PIA before developing or procuring the system, and the Office of Management and Budget (OMB) require the PIA to be submitted as part of IT budget requests. In Alberta, where PIAs are required under the Health Information Act, agencies are required to conduct the PIA and submit it to the Information and Privacy Commissioner for "review and comment" prior to implementing any new initiative. If a PIA is a prerequisite to starting a project, there is a danger that it won't be revisited during the project and that the final project may differ from what was originally proposed.

3.2.11 Stakeholder Consultation

All of the handbooks stress the importance of stakeholder consultation during the PIA and stakeholder communication following the PIA. The idea is to understand the potential privacy risks from their perspective and not just from the perspective of the organisation developing the initiative. One of the checklist entries in the Ontario handbook asks "Where appropriate, have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the proposal?" The Canadian and Ontario handbooks describe the PIA report as a communications tool for use with stakeholders, though additional types of communication might also be considered, e.g. reports targeted at specific stakeholder groups.

The UK handbook places great emphasis on stakeholder consultation and analysis and notes "By actively seeking out and engaging the concerns of stakeholders, even those who are expected to oppose a particular project, you can discover the reasoning behind their position and identify where further information needs to be provided and pre-empt any possible misinformation campaigns by opponents of the project." It also warns that stakeholder analysis needs to take place early on in the initiative so that it can genuinely affect it, otherwise it risks raising unrealistic expectations.

3.2.12 Health Guidelines

In addition to general PIA handbooks both Alberta and Ontario have separate PIA guidelines for health information initiatives (Alberta Health and Wellness, 2006, Ontario Information and Privacy Commissioner, 2005).

The Alberta Health Act requires "health information custodians" to conduct a PIA and to submit the report to the privacy commissioner before the new or revised health initiative is implemented. In

Ontario the Health Act requires organisations that provide services to two or more health information custodians to conduct a PIA and to provide the report to those custodians, but there is no requirement to provide the PIA report to the privacy commissioner. The Ontario guidelines recommend that other health information custodians carry out PIAs for new or revised programmes.

In both Alberta and Ontario a questionnaire is provided that provides the basis of the PIA report. The Alberta questionnaire is a standard questionnaire used for all PIAs in that jurisdiction, not just those related to health information. The Ontario questionnaire is specific to the Health Act. The questionnaires have similar formats: a series of questions about the organisation's structure and policies for privacy management, followed by a series of questions related to the initiative in question. As well as answering the questions the PIA team are expected to enclose supporting documents such as privacy policies, data flow diagrams and security policies.

The topics covered in these guidelines for health information are largely the same as those for any PIA, i.e. the authority to collect the data, identifying the purposes for the data collection, patient consent to capture and use the data, patient access to view and correct the data, stakeholder consultation, safeguards around data linking and data disclosure, and security policies and procedures.

The Alberta guidelines state that the health information data elements should be grouped into registration, diagnostic, treatment and health services provider information. The Alberta guidelines also include specific questions about the authority to use the personal health number, linkages to other systems, disclosure of health information and data matching. The questionnaire also asks whether the system will log all accesses of health information. The Ontario guidelines emphasise the importance of senior executive involvement in the development and implementation of privacy programs.

Both sets of guidelines include questions on trans-border movement of health information to establish whether the information will be adequately protected in other jurisdictions.

The Victoria handbook and supporting documents make reference to the Victorian Health Act 2001, where appropriate (Office of the Victorian Privacy Commissioner, 2009b).

3.2.13 Review of Screening Tools

Not all projects warrant a PIA, so several of the PIA handbooks include a screening or threshold assessment tool to determine whether or not one is required. These vary in format – the most common format is a series of around ten yes/no questions, where a 'yes' answer indicates that a PIA is required. In Canada, where PIAs are mandatory for new programs and services, the Ministry of

Government Services (MSG) in Ontario has developed a screening tool which is submitted to the privacy office, who evaluate and decide whether a PIA is required or not. The MSG screening tool has open questions rather than yes/no questions, since the responses are evaluated by the privacy office. Jurisdictions, such as the US, that do not have a threshold assessment do include a descriptive checklist of the types of projects that would require a PIA. The UK handbook has two threshold assessments – one for a full-scale PIA, and one for a small-scale PIA. The UK threshold assessment for a full-scale PIA runs to 8 pages and categorises the questions as follows:

- Technology
- Justification
- Identify
- Multiple Organisations
- Data (personal data)
- Data Handling
- Exemptions

It also provides background information on each of the categories of question.

A questionnaire type threshold assessment has advantages over a descriptive list of the types of projects that require a PIA. First, there is a record of the threshold assessment being carried out and a decision being made on whether to carry out a PIA or not. Second, the act of filling out the questionnaire is more likely to result in the consideration of privacy issues that reading a descriptive list. Finally, any privacy issues are more likely to be considered earlier in the project, which is one of the goals of PIAs (Bennett and Raab, 2006, p.260). A one-page questionnaire has the advantage of clarity and simplicity, but for many organisations some background information is necessary in order for them to carry out the threshold assessment.

The table below summarises the types of screening tools available in other jurisdictions.

Jurisdiction	Type of screening tool
Ontario Ministry of Government Services	Brief description of project 14 open questions
Canada Treasury Board Secretariat	Descriptive checklist
US	Descriptive checklist
Victoria	17 yes/no questions
Australia	Brief description of project Single yes/no question
UK	Questionnaire for full-scale PIA: • 11 questions with background information and details of exemptions Questionnaire for small-scale PIA: • 15 questions with background information and details of exemptions

Table 1 – Types of Screening Tools

3.2.14 COMPARISON OF HANDBOOKS

This table summarises the features of the various handbooks reviewed.

Feature	Canada Alberta	Canada British Columbia	Canada Ontario	Canada	USA	Australia, Victoria V1	Australia, Victoria V2	Australia	New Zealand	UK V1	UK V2
Handbook	Yes	No Web Page	Yes	Yes	No Memorandum on eGovt Act 2002	Yes	Yes	Yes	Yes	Yes	Yes
Published	2001	2006	2001	2002	2003	2004	April 2009	2006	2007	2007	June 2009
Words	13,295	994	25,000 approx	8,262	7,767	11,440	9008	17,355	11,389	33,320	22,923
Pages	36	7	96	40	18	36	28	51	44	113	81
Mandatory	**Yes** in Health Information Act 2001	**Yes**, for Government Institutions	No	**Yes**, for most Government Institutions	**Yes** for eGovernment projects	No	No	No	No	No	**Yes**, for Central Government and its agencies
Threshold Assessment	No	No	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Guide to Information Privacy Principles (IPPs)	No	No	Yes	No	No	Yea	No (but included in separate document)	No	Yes	No	No
Process Overview	No	No	Yes	Yes	Yes	No	No	Yes	Yes (brief)	Yes	Yes
IPP Compliance Checklists	No	No	Yes	Yes	No	Yes	No (included in separate document)	Yes	No	Yes	Yes
Report Outline	No (questionnaire provided)	No (questionnaire provided)	No (questionnaire provided)	Yes	Yes	No	Yes (in separate 63 page document)	No	Yes	Yes	Yes

Table 2 - Comparison of Handbooks

3.2.15 Publication of PIAs

There are many reasons put forward for the publication of PIA reports. Firstly, it reassures the public and privacy advocates that privacy issues have been considered. Secondly, it allows privacy advocates evaluate the decisions that were taken. Thirdly, the published PIA reports are a resource for other agencies, possibly in other countries, telling them how the privacy risks of certain types of initiatives have been handled in other countries. The UK handbook recommends doing an environmental scan at the start of a PIA to "to seek out information about prior projects of a similar nature", so the availability of published PIA reports would assist this process. The benefits of publication need to be balanced against any additional security risks that could arise as a result of making available details of the privacy risk analysis and mitigation.

In Canada government agencies are required to make summaries of PIA reports available online. The US e-Government Act requires agencies to publish PIA reports, where security considerations allow. Privacy commissioners in Australia have recommended that PIAs are published to protect the reputation of the Government and to act as a reference to others undertaking similar initiatives (Australia Office of the Privacy Commissioner, 2006). In most jurisdictions PIA reports, or summaries, may be accessed via Freedom of Information legislation.

3.3 Review of Published PIA Reports

It can be difficult to assess whether PIAs achieve their goals, when the impacts, positive or negative, may be many years into the future. Clarke (2008) states that "the coming years will tell whether PIAs achieve their aims of surfacing issues, involving the public, and ensuring a multi-stakeholder approach to initiatives".

The author reviewed three published PIA reports to see whether they achieved the aims of a PIA. The first has been published since the publication of the UK PIA handbook. This is *The Review of Domestic Rating Data Sharing Privacy Impact Assessment* by the Department of Finance and Personnel in Northern Ireland (Northern Ireland, 2008). The proposed initiative was to share data between the Social Security Agency and the Land Property Services in Northern Ireland to improve the take-up of certain benefits and to assess claims for housing benefits. The PIA report fails to include some of the suggested sections recommended in the UK handbook, e.g. an analysis of privacy issues and a discussion of alternatives considered, and in fact does not identify any significant privacy issues. Also, although there was a public consultation phase, there is no summary of the issues raised and responses to these.

The second PIA report reviewed was for the Introduction of a Western Australia Government Number (WAGN), which was a project to introduce a unique identifier for Government employees

(Clayton Utz, 2007). The PIA was carried out by a private consultancy in accordance with the Australian PIA guidelines. The report starts with an executive summary which clearly sets out the background to the project and the recommendations that came arose from the PIA. The seven recommendations range from technical (to limit access to the system) to procedural (to develop a code of conduct for operating the system) to legislative (to consider regulations to restrict private sector collection or use of the WAGN). The report is extensive and provides both background information on the PIA approach and the stakeholder consultation.

The third PIA report reviewed was an executive summary of a PIA for the Canadian Forces Health Information System (CFHIS) Project (PAKEMAN and Associates, 2004). This report is structured around the ten principles of fair information, and describes any risks identified and how they will be avoided or mitigated.

A review of privacy in the area of Shared Services carried out in Ontario found that privacy breaches were not systemic problems but as a result of unrelated issues to do with security, training and technology (Deloitte and Touche LLP, 2005). This review looked a number of PIAs and found that while most of the PIAs included detailed descriptions of the personal information involved, they were lacking in a number of areas:

- The privacy analysis was at too high a level
- They did not adhere to the guidelines for PIAs
- They hadn't been updated when the systems were subsequently updated
- They focused too much on technology and not the full business process.

The review recommends that PIAs be made mandatory for any change to a process that collects or uses personal information; that organisations adopt a privacy culture; and that responsibility for privacy should be centralised within an organisation or government department.

3.4 IRISH CONTEXT

While there are no guidelines on PIAs in Ireland at present, there are a number of other publications that provide assistance.

The Office of the Data Protection Commissioner (ODPC) has published guidelines on *Biometrics in the Workplace* (Data Protection Commissioner, 2007) and *Biometrics in Schools, Colleges, and Other Education Institutions* (Data Protection Commissioner, 2009). The guidelines are designed to be used in advance of the introduction of a biometric identification system to allow organisations "to fully

consider if there is need for a biometric system in the first place and then to assess the privacy impact of different systems". The guidelines provide useful background information on biometrics, highlight the relevant data protection concepts, and provide a checklist of questions to be considered in the context of a privacy impact assessment. The advantage of focussed guidelines like these is that the team carrying out a PIA does not have to wade through pages of guidelines to find those that are relevant to their own initiative.

The ODPC has also published various guidelines for the health sector covering areas such as consent, research, and the transfer of patient records between organisations. In addition the ODPC has formally approved codes of practice developed by three industry sectors: the Garda Síochána, the Injuries Board and the Insurance sector.

3.5 Critics of PIAs

The majority of the contributors of articles and reports about PIAs are either privacy commissioners or privacy consultants, who tend to be advocates of this approach. There are very few studies or articles criticising the PIA approach though a few authors have pointed out some of the limitations. Hope-Tindall (2002) warns against "a compliance mentality view of the PIA as yet another hurdle to be overcome in the already cumbersome project and funding process". He proposes a three-pronged approach to address this, comprising a 'Privacy Framework', a 'Privacy Impact Assessment' and a 'Privacy Architecture'. The Privacy Framework contains the legislation, guidelines and directives that are relevant to the project in hand, and an environmental scan of similar initiatives in other organisations or countries. It acts as a kind of privacy constitution for the project and can be used for early review by the privacy commissioner. The Privacy Architecture addresses the technical and design issues and the solutions to these. The Privacy Impact Assessment addresses the non-technical and policy issues and solutions. He recommends that both the PIA and Privacy Architecture are "both active and responsive" by which he means that opportunities to introduce privacy enhancing policies and technology are actively sought out. It could be argued that all the elements of a Privacy Framework and Privacy Architecture are part of a traditional PIA, though separating them into individual documents may give greater emphasis to areas such as technical solutions.

Kenny and Borking (2002) criticise the non-technical nature of PIAs, saying that they are based on legal rather than technical principles and that they lead to "descriptive" rather than "prescriptive" recommendations. It is true that most PIA handbooks are based around the principles contained in the relevant privacy legislation and so, if the right skills are not included in the PIA project team, technical security and privacy issues may be overlooked. Kenny and Borking propose an alternative approach whereby the relevant legislation is distilled into technical requirements or "work items".

For example, the principle that “the data subject should be aware of the uses of their personal data” would be translated into a series of work items such as: “Before the data are collected, the data subject is informed of: identify of controller and Purpose Specification for which the data are intended”.

The US based Open Security Foundation (www.datalossdb.org) tracks statistics for each major privacy breach reported to it (Open Security Foundation, 2009). They report that 68% of privacy breaches are initiated by people external to the organisation, and the most frequent types of privacy breach are: stolen laptop (21%), hacking (17%), Web based data loss (11%) and stolen computer (7%). The PIA process typically concentrates on the legitimate procedures for capturing and processing personal data rather than illegitimate or fraudulent procedures. While a PIA handbook may include questions such as “Have security procedures for the collection, transmission, storage, and disposal of personal information, and access to it, been documented?”(Ontario Information and Privacy Office, 2001) it is questionable if this will prompt a detailed review of data security which would prevent the types of data losses listed above.

4 DESIGN OF PIA HANDBOOK

This section describes how the PIA handbook for the Irish Health Sector was designed by the author.

4.1 DESIGN OF THRESHOLD ASSESSMENT TOOL

A questionnaire type threshold assessment tool was included in the Irish PIA handbook as it is an easy way for an organisation to get started on assessing privacy issues. A yes/no type questionnaire was selected as this is the simplest to fill out and it results in a clear-cut decision on whether to carry out a PIA or not.

The threshold assessment tool starts with some simple questions on whether the initiative involves the collection, use, or disclosure of personal information. It follows with more probing questions about technology considerations, the use of new or existing identifiers, and data sharing across organisations. It finished with an open question about whether the initiative is likely to raise any privacy concerns with the public. While the questions are short, each question has background information for those less familiar with privacy issues.

The questions have been categorised, similar to the UK threshold assessment, as this encourages the PIA team to take a broader look at an area, rather than simply answering each yes/no question in turn.

4.2 DESIGN OF PIA HANDBOOK

The design of the PIA Handbook involved reviewing the handbooks from other jurisdictions to pick the best aspects of each, and then tailoring it for the Irish context and health sector.

There were a number of considerations when designing the handbook. Above all that it should provide a clear framework on how to carry out a PIA, including who should be involved, the activities to be carried out, the timing and sequencing of these and the issues to be considered. Given that at PIAs are new to Ireland and that they are not yet mandatory, it was felt that a “light touch” approach was appropriate, meaning that the handbook should not be overly long or prescriptive. This approach was also recommended by the Deputy Data Protection Commissioner (Gary Davis, 2009).

The audience for the handbook will include a wide range of people, including those who are familiar with privacy principles and those that are new to them. To handle this, the handbook was designed to give summary information for experienced users with additional background information for less experienced users, and links to other resources, for those that were interested.

The structure of the handbook is based on the Australian, New Zealand and Ontario handbooks. It starts with the rationale for doing a PIA and the potential benefits. It goes on to explain the concept of privacy. Next it explains how to prepare for and carry out the PIA. Then it describes the typical outline of a PIA report. While this outline might not be appropriate for all PIA reports it is useful for groups undertaking a PIA for the first time, and as a way of ensuring that important aspects of a PIA are not omitted.

The overview diagram in section 1.5 of the handbook (shown below) was adapted from a diagram in the New Zealand Handbook which shows how the PIA activities take place in parallel with system development (New Zealand Privacy Commissioner, 2007).

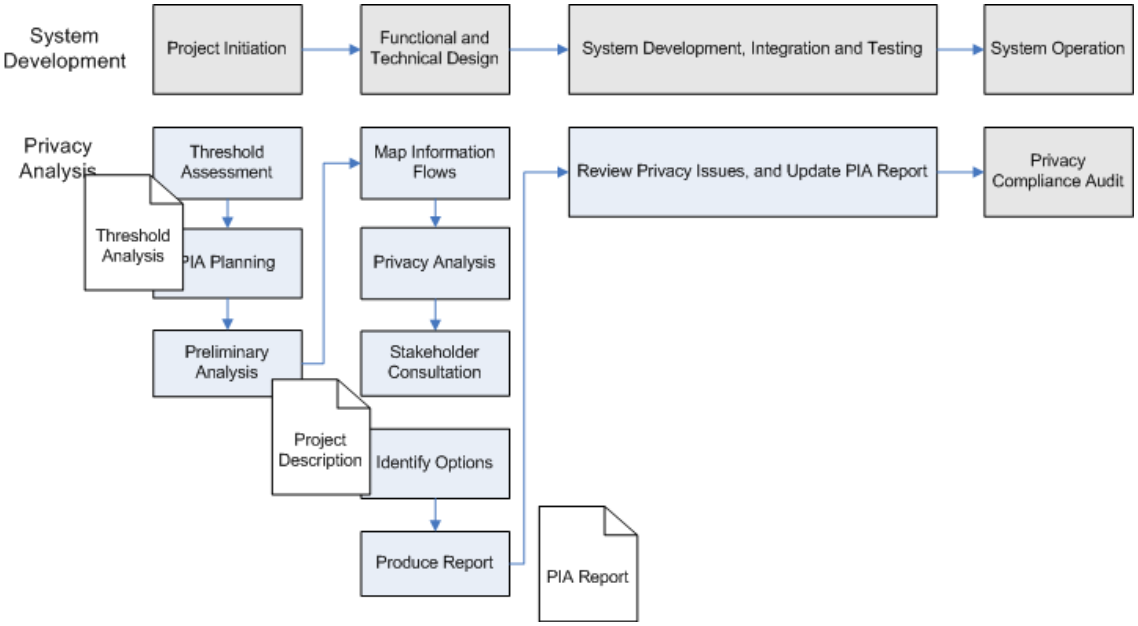


Table 1 - PIA Process Overview

The final and largest section of the handbook is a series of compliance checklists. The checklists and much of the related background information were copied directly from the Office of the Data Protection Commissioner website, with the permission of that office (Office of the Data Protection Commissioner, 2008a). An additional checklist was added to cover Freedom of Information requirements. Additional items were added to each checklist to cover health information considerations. These were taken from a list of Health Information Principles published as part of the consultation process on the Health Information Bill to be published in 2009 (Department of Health and Children, 2008a).

4.3 DESIGN OF ELECTRONIC PIA HANDBOOK

The handbook was first written as a Microsoft Word document and then converted to an electronic form to allow greater ease of use. The product chosen to develop the electronic handbook was Microsoft Infopath, which is an electronic forms designer that is part of the Microsoft Office suite. This product was chosen because it provided all the necessary features such as validation of data elements and conditional logic. In addition it is widely available, and unlike many other forms processors it can operate in a standalone mode without the need for an application server.

Though the electronic form version of the handbook contains the same information as the Word document, the objective was to provide greater ease of use through a number of features:

- Hyperlinking of key term to definitions and to allow navigation through the document
- The ability to hide or display background information through the click of button
- Marking some fields as mandatory to ensure completeness of the responses.

5 APPLICATION OF PIA

The author chose a project for a Government department that carries out medical assessments to evaluate the PIA handbook. The project is to review and redesign the business processes and organisation structure for both medical assessments and administrative functions; to develop systems to support the future business processes, and to develop evidence based medical protocols for the assessments.

The project is being undertaken by BearingPoint Ireland, the author's employer, and she is a member of the project team acting as an IT business analyst. The project started in February 2009, and is due for completion in October 2010, with a series of intermediate releases, the first of which is scheduled for September 2009.

The author has worked for over five years on similar, though not health related projects, for the same department. Although risk assessment was a normal part of the project management practices for these projects this risk assessment did not typically include consideration of privacy risks.

5.1 PIA PLANNING

The author approached the project sponsor to suggest the idea of carrying out a PIA on the project. The project sponsor, who is also the data controller for this section of the department, was receptive to the idea and so a number of activities were scheduled to carry out the PIA. These are listed below:

17 April 2009	Introductory sessions with the project sponsor and members of the Information Services Unit who are responsible for data security and data protection.
Week starting 23rd March 2009	Write short project description
24th April 2009	Workshop 1: Introductory Session with Project Team, and Preliminary Privacy Analysis
30th April 2009	Workshop 2: Map Information Flows and Assess Privacy Risks
Thursday 14th May 2009	Workshop 3: Agree approaches to handling Privacy Risks
Week starting 18th May 2009	Write PIA Report
Week starting 18th May 2009	PIA participants to complete Evaluation Forms

Table 2 - PIA Schedule of Activities

5.2 PIA PROCESS

5.2.1 INTRODUCTORY SESSION

The first meeting was a short session with the project sponsor and a member of the Information Services Unit (ISU). The ISU are responsible for data protection and security within the department. They run a variety of training and awareness programmes which are mandatory for all staff, including temporary workers. The purpose of this meeting was to introduce the concepts behind a PIA and to get the support of the ISU. The representative from the ISU agreed to attend all subsequent workshops.

A meeting with the head of the ISU was also requested to discuss the PIA and to get his views. Although the meeting was scheduled it was subsequently postponed and did not take place during the research project.

5.2.2 FIRST WORKSHOP – PRELIMINARY PRIVACY ANALYSIS

The first workshop was held with the project sponsor, the project team, the representative from ISU and another member of the BearingPoint consultancy team who is responsible for the future process and organisation design aspects of the project. There were a total of nine people including the author. The author explained the purpose of the PIA, the proposed approach and gave an overview of the "fair information" principles contained in the Data Protection Acts. Each attendee was given a printed copy of the PIA handbook that was developed as part of this research project. The project sponsor informed the group that because of her grade within the department that she is regarded as a data controller. It was not felt necessary to do a threshold assessment since the project clearly fell within the category of projects that would benefit from a PIA.

The intention had been to use the Infopath version of the handbook during the PIA. However, due to technical reasons (an incompatible PC), a printed version of the Word document was used instead, supplemented by a PowerPoint presentation.

The introduction was followed by a preliminary privacy analysis. This took the form of a review the high level business processes with a view to identifying any potential privacy risks. The review used high-level process maps that had previously been documented as part of the project. Ten privacy risks were identified, relating both to patients and the doctors who carry out the assessments. The types of privacy risks identified included the following:

- The new system will capture medical assessments electronically and additional medical reports will be scanned and linked to the patients details. The move from paper-based to

electronic records could potentially lead to far greater access to medical information if the appropriate security and access controls are not put in place.

- The amount of personal data collected about each doctor was questioned. In particular the need to capture the doctor's PPSN was questioned. Since the PPSN is used as a personal identifier in many Government departments the availability of the PPSN could lead to privacy breaches.

Each privacy risk was discussed to identify possible ways of avoiding or mitigating the risk. For a couple of the privacy risks the project team members agreed to do further investigation as to why certain personal information was captured, with a view to not capturing it in future if this was not required. Towards the end of the workshop it was agreed that one of the outcomes of the PIA would be a set of privacy design principles to be used throughout the rest of the project.

After the workshop the author documented and circulated a preliminary privacy impact assessment report.

5.2.3 Second Workshop – Detailed Privacy Analysis

A second workshop was held a week later with all but one of the same attendees. According to the handbook and the pre-arranged schedule this workshop should have performed a detailed privacy analysis based on detailed data flow diagrams. However the consensus was that this would not identify any further privacy risks. The detailed data flows had been documented by the project team in advance of the first workshop as part of the process design aspect of the project, and it was felt that the discussions at the first workshop took into account the detailed process flows since most of the participants were very familiar with them. Therefore the second workshop revisited the privacy risks identified in the first workshop and attempted to identify options for each of these and to extend the list of privacy design principles. While options were found for most of the privacy risks it became clear that the project team did not represent all of the stakeholder groups within the Department and that further meetings would need to be arranged to discuss the options for some areas, and to get buy-in for the privacy design principles.

Following the second workshop the author updated and re-distributed the preliminary privacy impact assessment report. At this point the project sponsor requested that the preliminary and final reports would not be made public and so they have not been included in this dissertation.

5.2.4 *Third Workshop – data Protection Checklists*

The third workshop went through the data protection and freedom of information checklists at the back of the handbook. A "no" answer to any of the checklist questions would indicate that there was a privacy risk. The answer to the majority of questions was "yes". The process of going through the checklists lead to a number of discussions:

- How was the data used, and which uses could be considered "primary" and which "secondary"
- Whether explicit consent was required to use the data for research and statistical purposes
- Whether data was sent to any external bodies.

The workshop also identified areas where security procedures were in place but were not fully documented. The outcome of the discussions was an expanded list of "design principles" to be followed in later phases of the project.

After the workshop the author established that the use of the data for internal research and for statistics was allowed. The author then documented a full privacy impact assessment report, which was reviewed by the project sponsor. The report was then made available within the department.

5.3 Limitations

The limitations of the PIA and evaluation must be acknowledged:

- The number of participants was small and all except two came from the same section within the department,
- The ongoing working relationship with the author may have lead participants to give more favourable responses that if the author had been unknown,
- The department is not typical of health care organisations,
- The evaluation of the handbook was based on a single PIA,
- The handbook was not used in isolation: the author lead the workshops and used a presentation to introduce the topic and guide the process.

Nevertheless, the author believes it was a worthwhile exercise to evaluate the process and handbook, both from the research point of view, and for the department to reflect upon the benefits of this approach and its potential use on future projects.

5.4 Design of Evaluation Form

Each of the participants in the PIA process was invited to complete an anonymous evaluation form (see Appendix B). The results are summarised in Section 5.5.

The purpose of the evaluation was twofold: firstly to see if the PIA achieved its objectives and was of benefit to the project, and secondly to evaluate the usefulness of the handbook.

The evaluation form was designed as a structured self-completed questionnaire, delivered through the SurveyMonkey website (www.surveymonkey.com). This method was selected as it is a quick, anonymous and avoids interviewer bias. The questions are a mixture of pre-coded questions to allow for analysis of the results, and open ended questions so as not to attempt to anticipate all of the possible responses.

The evaluation form has three parts. The first part of the evaluation asks the participant to judge how well the PIA achieved the benefits listed in section 1.2 of the handbook ("Why do a PIA?"). The next part asks the participants about their views on the PIA process and the potential for involvement of the Data Protection Commissioner in the process. The final part asks for views on the PIA handbook and how it could be improved.

5.5 Survey Results

This section summarises the results from the evaluation form survey. Seven out of the eight participants in the PIA completed the evaluation form.

5.5.1 Benefits of doing a PIA

The first question was about the benefits of doing the PIA. All participants agreed with the following benefits of the PIA:

- Avoids costly system modifications after go-live
- Avoids privacy breaches and the resulting loss of confidence
- Builds trust and increases the acceptance of the initiative
- Avoids negative publicity
- Develops a privacy aware culture within the organisation
- Explains how privacy risks have been balanced against other factors.

All participants except one agreed with the following benefits:

- Ensures compliance with legislation
- Promotes informed decision making

The results are shown in table 5 below.

Potential Benefit	**Strongly Agree**	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Avoids costly system modifications after go-live	29% (2)	71% (5)	0	0	0
Avoids privacy breaches and the resulting loss of confidence	43% (3)	57% (4)	0	0	0
Builds trust and increases the acceptance of the initiative	33% (2)	67% (4)	0	0	0
Avoids negative publicity	14% (1)	86% (6)	0	0	0
Ensures compliance with legislation	28% (2)	57% (4)	14% (1)	0	0
Develops a privacy aware culture within the organisation	14% (1)	86% (6)	0	0	0
Promotes informed decision making	0	86% (6)	14% (1)	0	0
Explains how privacy risks have been balanced against other factors.	43% (3)	57% (4)	0	0	0

Table 3 – Benefits of a PIA

5.5.2 VIEWS ON THE PIA PROCESS

The next section was designed to get the views of the participants on the PIA process and to find out if they felt it was beneficial in uncovering privacy risks.

All participants thought the PIA uncovered privacy risks that might not otherwise have come to light and all intended using this approach on future projects or enhancements to the current project. All bar one thought the process identified ways to address the privacy risks. One participant suggested that “it would be useful to list who is responsible for each of the risks identified”.

The results are shown in Table 6 below.

Question	Yes	No	Don't Know
Did the process uncover privacy risks that might not have come to light?	100% (7)	0	0
Did the process help in identifying options to address those privacy risks?	86% (6)	14% (1)	0
Would you use this approach on future projects or on enhancements to this project?	100% (7)	0	0

Table 4 – Views on the PIA Process

5.5.3 Stakeholder Consultation

The next question was designed to find out if the participants thought that the stakeholder consultation was sufficiently broad based. Stakeholder consultation is considered an important part of the PIA process, including consultation with those that may oppose the project.

57% (4) of the respondents thought the necessary stakeholders were involved or consulted on the PIA process, 29% (2) thought that all the necessary stakeholders were not involved and 14% (1) did not know.

The comments in relation to stakeholder involvement were diverse: One participant said "(For good reasons) the actual data owners (e.g. patients & doctors were not consulted). So we just assumed what they think". Two other participants added comments to suggest that there should have been wider stakeholder involvement in the process.

5.5.4 Involvement of Office of the Data Protection Commissioner

The next question was designed to find out if the participants would be willing to make the PIA report available to the Office of the Data Protection Commissioner if that office was conducting an audit or investigation of the section. One of the reasons that privacy offices in other jurisdictions promote PIAs is that the availability of a PIA report makes their investigations easier and more effective.

All 7 participants responded that they would make the PIA report available to the Office of the Data Protection Commissioner in this situation. One participant commented that it was "best to be very up-front and show an effort in a complicated area."

5.5.5 *PUBLICATION OF THE PIA REPORT*

The next question asked if the participants thought it would be a good idea to make the PIA report or a summary of the report publicly available. The publication of PIA reports or summaries is mandatory in some jurisdictions and even where it is not mandatory it is considered good practice in order to increase public confidence.

Views were split on whether it would be a good idea to make the report or summary publicly available? 43% (3) of participants responded Yes, 43% (3) responded No, and 14% (1) was undecided. One reason given for making the report public was that it "would help to give confidence that the issue is being addressed". Reasons for not making the report public were more around uncertainty of the public reaction to this, rather than outright opposition to publication. One participant wrote that they "would like to see more of this by this Department and other Departments before we went down this route".

5.5.6 *VIEWS ON HANDBOOK*

The next section was designed to get the views of the participants on the PIA handbook.

100% (7) of participants responded that they found the handbook easy to follow, that the background information was of a suitable level and that the questions were relevant to the project. 43% (3) were familiar with privacy principles before starting the PIA while 57% (4) were not familiar.

Question	**Yes**	**No**	**Don't Know**
Did you find the handbook easy to follow?	100% (7)	0	0
Were you familiar with privacy principles before starting the PIA?	43% (3)	57% (4)	0
Did you find the background information to be of a suitable level?	100% (7)	0	0
Were the questions relevant to your project?	100% (7)	0	0

Table 5 – Views on the PIA Handbook

The participants were also asked which section of the handbook they found the most useful. 57% (4) said the introduction to privacy concepts was the most useful and 57% (4) said the checklists related to data protection and FOI was the most useful. The overview of the PIA process was not selected as "most useful" by any participant.

Section	**Yes**
Introduction to privacy concepts	57% (4)
Overview of PIA process	0
Checklists related to data protection and FOI principles	57% (4)

Table 6 – Most Useful Sections of PIA Handbook

5.5.7 General Comments

The final section asked the participants for any other general comments on the process or handbook.

The comments included suggestions that someone should have a "'privacy hat' on at future workshops"; that the current (pre-project) privacy situation should be evaluated and compared with the situation after the system went live; and that bullet point guides should be developed for the future users of the system.

5.6 Discussion on PIA

The reason for doing the PIA was to assess the actual benefits of a PIA on a real project. It is clear from the evaluation that the PIA was beneficial. It did identify several privacy risks that might not have come to light or that may only have emerged later in the process when they were more costly to address. The PIA allowed for a detailed discussion of these risks in the context of risk assessment and compliance with data protection and other legislation. The discussions led to options for mitigating or avoiding the risks. The outcome of the PIA was a set of design principles that have implications for both the system and business processes that will be carried forward to future phases of the project.

It became clear to the author during the PIA that the stakeholder consultation during the PIA was not wide enough, for example there was no consultation with patients, patient representative groups, or the doctors who carry out the medical assessments. This limitation was only recognised by 29% of the participants. This is likely to be partially addressed in future phases of the project to the extent that the doctors will be included in discussions, but earlier involvement of a broader range of

stakeholders would have been desirable and would have made the PIA report representative of a broader range of viewpoints.

Privacy offices, including the Office of the Data Protection Commission (ODPC), encourage organisations to consult with them on privacy and data protection issues. While all of the participants indicated that they were willing to provide the final PIA report to the ODPC there was a reluctance to consult with that office during the PIA process, though it was suggested by the author a couple of times where there were diverging viewpoints or lack of clarity over the legal situation.

One of the main reasons for doing a PIA is to increase public confidence in new initiatives particularly where new technology is involved. Only 43% of the participants thought that the PIA report should be made publicly available. The reason for this was uncertainty about the public reaction and not wanting to be the first organisation in Ireland to do this.

The proponents of PIAs argue that it is more cost effective to identify privacy risks early on in a project, rather than later when there has been a significant investment. While there was no attempt to do a detailed cost/benefits analysis, some simple calculations would indicate that it was cost effective. The total effort involved in the PIA was approximately 15 person days (2 days preparation, 9 days for workshops and 4 days for writing the report). The cost of a single privacy breach or system feature redesign would far exceed this. However, the effort to do the PIA was less that it might have been on other projects because almost all the participants were already involved and familiar with the project and many of the artefacts required, such as process maps and data flow diagrams, were already available.

6 CONCLUSIONS AND FUTURE WORK

The aim of the research project was to develop a PIA handbook geared to the health sector in Ireland and to evaluate it based on its application to a real project. The development of the handbook involved reviewing PIA handbooks from other jurisdictions, data protection guidelines in Ireland and background information on the forthcoming Health Information Bill. The handbook was then used to carry out a PIA on a real project. The effectiveness of the PIA and handbook were evaluated by a survey of the PIA participants.

The PIA was found to be beneficial to the project. It identified privacy risks that might not have come to light otherwise and led to the development of privacy design principles for the project. The handbook was found to be useful as an introduction to privacy principles and as a way of guiding the process. Some limitations were found due to restricted stakeholder consultation and the fact that the PIA was initiated by the author rather than the organisation responsible for the initiative.

The results showed that a PIA is an effective approach to protecting privacy that complements other measures such as an information security assessment. However a PIA is only effective if it is conducted early on in an initiative when it can affect the outcomes; where there is meaningful engagement between the organisation responsible for the initiative and stakeholder groups; and where the organisation takes ownership of the PIA and reviews it periodically.

There is much further work that could be done in this area. Firstly, once the Health Information Bill is passed and regulations concerning PIAs are brought into affect, the handbook should be updated to reflect these regulations. Secondly, the handbook would also benefit from more extensive guidance on health information and technology issues. Thirdly, the health specific information could be removed to develop a general purpose handbook, for use with other types of initiative. Finally, a detailed annotated PIA report outline would be a useful tool for those carrying out PIAs.

PIAs are likely to become part of the landscape for health information initiatives in Ireland over the next few years. It is hoped that organisations engage in the PIA process in a meaningful way so that advances in health information are accompanied by enhanced privacy protection.

REFERENCES

AGRAWAL, R. & JOHNSON, C. (2007) Securing electronic health records without impeding the flow of information. *International Journal of Medical Informatics,* 76**,** 471-479.

ALBAN, R. F., FELDMAR, D., GABBAY, J. & LEFOR, A. T. (2005) Internet security and privacy protection for the health care professional. *Current Surgery,* 62**,** 106-110.

ALBERTA (2006a) Freedom of Information and Privacy Compliance Guidelines. *Available at http://foip.alberta.ca/resources/guidelinespractices/chapter9.cfm (Accessed: 1 March 2009).*

ALBERTA HEALTH AND WELLNESS (2006) Health Information Act Guidelines and Practices. *Available at: http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf (Accessed: 31 July 2009).*

ALBERTA (2001) Privacy Impact Assessment: Instructions and Annotated Questionnaire. *Available at: http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf (Accessed: 31 July 2009).*

AN BORD ALTRANAS (2000) The Code of Professional Conduct for each Nurse and Midwife.

AUSTRALIA OFFICE OF THE PRIVACY COMMISSIONER (2006) Privacy Impact Assessment Guide. *Available at: http://www.privacy.gov.au/publications/PIA06.pdf (Accessed: 27 September 2008).*

BBC NEWS (2008) Timeline: Child benefits records loss. *Available at: http://news.bbc.co.uk/2/hi/uk_news/politics/7104368.stm (Accessed: 23 November 2008).*

BENNETT, C. & RAAB, C. (2006) *The Governance of Privacy,* Cambridge, The MIT Press.

BRENNAN COMMISSION (2003) Commission on Financial Management and Control Systems in the Health Service.

BRITISH COLUMBIA OFFICE OF THE CHIEF INFORMATION OFFICER (2006) Privacy Impact Assessment Process. *Available at http://www.cio.gov.bc.ca/services/privacy/Public_Sector/pia/default.asp (Accessed: 1 January 2009).*

CANADA MINISTRY OF GOVERNMENT SERVICES (2008) Freedom of Information and Privacy Compliance Guidelines. *Available at http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.pdf (Accessed: 15 March 2009).*

CANADA TREASURY BOARD SECRETARIAT (2002) Privacy Impact Assessment Policy. *Available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450&section=text#sec6.5 (Accessed: 23 January 2009).*

CARTER, M. (2000) Integrated electronic health records and patient privacy: possible benefits but real dangers *Available at http://www.mja.com.au/public/issues/172_01_030100/carter/carter.html (Accessed: 15 March 2009)*

CLARKE, R. (2006) What's Privacy? *Australian Law Reform Commission on 28 July 2006* Available at http://www.rogerclarke.com/DV/Privacy.html (Accessed: 15 March 2009).

CLARKE, R. (2008) Privacy Impact Assessment: Its Origins and Development *Available at: http://www.rogerclarke.com/DV/PIAHist-08.html (Accessed: 1 March 2009).*

CLAYTON UTZ (2007) Proposed Western Australian Government Number PRIVACY IMPACT ASSESSMENT. *Available at: http://www.egov.dpc.wa.gov.au/Projects/IdentityAccessManagement/Pages/WAGNPrivacyImpactAssessmentReport.aspx (Accessed: 1 January 2009).* Western Australian Department of the Premier and Cabinet: Office of e-Government.

DATA PROTECTION COMMISSIONER (2007) Biometrics in Schools, Colleges and other Educational Institutions. *Available at http://www.dataprotection.ie/viewdoc.asp?DocID=409&ad=1 (Accessed: 25 March 2009).*

DATA PROTECTION COMMISSIONER (2008) Loss of Department of Social and Family Affairs information held by the Office of the Comptroller and Auditor General. *Available at: http://www.dataprotection.ie/viewdoc.asp?DocID=820&m=f*

(Accessed: 23 November 2008).
DAVIS,G. (2009) Personal interview. 2 February 2009.
DELOITTE AND TOUCHE LLP (2005) Ontario Shared Services Privacy Review. *Available at: http://www.gov.on.ca/MGS/graphics/052931.pdf (Accessed: 28 March 2009).*
DEPARTMENT OF HEALTH AND CHILDREN (2008a) Audit Of Key International Instruments, National Law And Guidelines Relating To Health Information For Ireland And Selected Other Countries. *Available at: http://www.dohc.ie/consultations/closed/hib/draft_audit_paper.pdf (Accessed: 23 March 2009).*
DEPARTMENT OF HEALTH AND CHILDREN (2008b) Discussion Paper of Proposed Health Information Bill. *Available at: http://www.dohc.ie/consultations/closed/hib/discussion_paper.pdf?direct=1 (Accessed: 3 May 2009).*
DEPARTMENT OF HEALTH AND CHILDREN (2008c) Public Consultation on Proposed Health Information Bill. *Available at: http://www.dohc.ie/consultations/closed/hib/ (Accessed: 23 March 2009).*
DEPARTMENT OF THE TAOISEACH (2008) The Public Service Broker Model.
FLAHERTY, D. H. (2002) Privacy Impact Assessments: an essential tool for data protection. *22nd Annual Meeting of Privacy and Data Protection Officials.* Venice.
FORTE, D. (2005) Spyware: more than a costly annoyance. *Network Security,* 2005**,** 8-10.
GOVERNMENT OF IRELAND (1988) Data Protection Act.
GOVERNMENT OF IRELAND (1989) Data Protection (Access Modification) (Health) Regulations.
GOVERNMENT OF IRELAND (1997a) Freedom of Information Act.
GOVERNMENT OF IRELAND (1997b) Health (Provision of Information) Act.
GOVERNMENT OF IRELAND (2003a) European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations.
GOVERNMENT OF IRELAND (2003b) Freedom of Information (Amendment) Act.
GOVERNMENT OF IRELAND (2005a) Disability Act.
GOVERNMENT OF IRELAND (2005b) Social Welfare Consolidation Act.
HOPE-TINDALL, P. (2002) Privacy Impact Assessment - Obligation or Opportunity: The Choice is Ours! *CSE ITS Conference.* Ottawa, Ontario.
HSE (2006) HSE Transformation Programme 2007- 2010. *Available at: http://www.hse.ie/eng/Publications/corporate/transformation.pdf (Accessed: 23 March 2009).*
HSE (2009) Hospital Co-Location Initiative. *Available at: http://www.hse.ie/eng/HSE_FactFile/HSE_Approach/National_Hospitals_Office/Hospital_Co-Location_Initiative_/ (Accessed: 31 July 2009).*
IAIA (2009) International Association for Impact Assessment. *Available at http://www.iaia.org/modx/ (Accessed: 1 March 2009).*
INFORMATION SOCIETY COMMISSION (2004) An e-Healthy State? *Available at: http://www.isc.ie/downloads/34842_e-healthy_state.pdf (Accessed 2 May 2009).*
IRISH MEDICAL COUNCIL (2004) Ethical Guide 6th Edition. *Available at: http://www.medicalcouncil.ie/_fileupload/standards/Ethical_Guide_6th_Edition.pdf (Accessed: 6 June 2009).*
KENNY, S. & BORKING, J. (2002) The Value of Privacy Engineering. *Available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny (Accessed: 14 March 2009).*
LENNON, P. (2005) *Protecting Personal Health Information in Ireland Law & Practice*, Oak Tree Press.
LENNON, P. (2009) Personal interview. 17 April 2009.
LIGINLAL, D., SIM, I. & KHANSA, L. (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security,* 28**,** 215-228.

LINDEN CONSULTING, I. (2007) Privacy Impact Assessments: International Study of the Application and Effects. IN OFFICE, I. C. S. (Ed.). London.
NEW ZEALAND PRIVACY COMMISSIONER (2007) Privacy Impact Assessment Handbook. *Available at: http://www.privacy.org.nz/privacy-impact-assessment-handbook/ (Accessed: 23 September 2008).*
NORTHERN IRELAND (2008) Review of Domestic Rating Data Sharing Privacy Impact Assessment (PIA). *Available at: http://www.ratingreviewni.gov.uk/data_sharing__pia.pdf (Accessed: 10 October 2008).* Department of Finance and Personnel.
OFFICE OF THE DATA PROTECTION COMMISSIONER (2008a) Data Protection Checklist. *Available at: http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3k.htm&CatID=55&m=y (Accessed: 10 April 2009).*
OFFICE OF THE DATA PROTECTION COMMISSIONER (2008b) Public Awareness Survey 2008. *Available at: http://www.dataprotection.ie/docs/Public_Awareness_Survey_2008/794.htm (Accessed: 31 July 2009).*
OFFICE OF THE DATA PROTECTION COMMISSIONER (2008c) Submission on the Proposed Health Information Bill. *Available at: http://www.dataprotection.ie/docs/Submission_of_the_Office_of_the_Data_Protection_Commissioner/900.htm (Accessed: 16 May 2009).*
OFFICE OF THE DATA PROTECTION COMMISSIONER (2009) Annual Report 2008. *Available at: http://www.dataprotection.ie/documents/annualreports/AR2008.pdf (Accessed: 23 May 2009).*
OFFICE OF THE NEW ZEALAND PRIVACY COMMISSIONER (2002) Privacy Impact Assessment Handbook. *Available at: http://www.privacy.org.nz/filestore/docfiles/48638065.pdf (Accessed: 15 March 2009).*
OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER (2004) Privacy Impact Assessments - A Guide. *Available at: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf (Accessed: 23 March 2009).*
OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER (2009a) Accompanying Guide to the Privacy Impact Assessment Report. *Available at: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/27FC495F3F506D49CA2575AC001305BE/$FILE/Accompanying%20Guide%20to%20OVPC%20PIA%20Template%20Report%20May%202009.pdf (Accessed: 3 July 2009).*
OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER (2009b) Privacy Impact Assessment Guide Edition 2. *Available at: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/B595F5F2FDFD2135CA2575AC0012BC0E/$FILE/OVPC%20Privacy%20Impact%20Assessment%20Guide%20Edition%202%20May%202009.pdf (Accessed: 3 July 2009).*
OFFICE OF THE VICTORIAN PRIVACY COMMISSIONER (2009c) Privacy Impact Assessment Report Template. *Available at: http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/61A2754F019EDA57CA2575AC001346F3/$FILE/OVPC%20PIA%20Template%20Report%20May%202009.doc (Accessed: 3 July 2009).*
ONTARIO INFORMATION AND PRIVACY COMMISSIONER (2005) Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act. *Available at: http://www.coptont.org/docs/Privacy/Privacy%20Impact%20Assessment%20Guidelines.pdf (Accessed: 31 July 2009).*
ONTARIO INFORMATION AND PRIVACY OFFICE (2001) Privacy Impact Assessment A User's Guide. *Available at: http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf (Accessed: 27 September 2008).*
OPEN SECURITY FOUNDATION (2009) Data Loss Statistics. *Available at: http://datalossdb.org/statistics (Accessed: 23 March 2009).*

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (2005) Statistics on Health Expenditure. *Available at: http://stats.oecd.org/WBOS/index.aspx (Accessed: 13 May 2009).*

PAKEMAN AND ASSOCIATES (2004) Preliminary Privacy Impact Assessment (PPIA) on the Canadian Forces Health Information System (CFHIS) Project *Available at: http://www.forces.gc.ca/health-sante/proj/CFHIS-SISFC/PPIA-EPFVP-eng.asp (Accessed: 14 March 2009).*

PONEMON INSTITUTE (2009) Gambling with Laptop Security. *Available at: http://www.ponemon.org/blog/post/gambling-with-laptop-security (Accessed: 23 May 2009).*

SECURITY MAGAZINE (2003) One third of firms hacked in 2003. *Available at: http://www.scmagazineus.com/One-third-of-firms-hacked-in-2003/article/30883/ (Accessed: 23 May 2009).*

SECURITY MAGAZINE (2008) Breach of Britney Spears patient data reported. *Available at: http://www.scmagazineus.com/Breach-of-Britney-Spears-patient-data-reported/article/108141/ (Accessed: 23 May 2009).*

SURVEILLANCE STUDIES NETWORK (2006) A Report on the Surveillance Society For the Information Commissioner. *Available at: http://www.dataprotection.ie/docs/A_Report_on_the_Surveillance_Society_For_the_Information_Com/386.htm (Accessed: 7 June 2009).*

T J MACINTYRE (2009) Bord Gais Laptop Loss. *Available at: http://www.tjmcintyre.com/2009/06/bord-g.html (Accessed: 4 July 2009).*

THE IRISH TIMES (2009) Bord Gáis failed to say stolen laptop data not encrypted. *Available at: http://www.irishtimes.com/newspaper/ireland/2009/0619/1224249119832.html (Accessed: 20 June 2009).*

UK CABINET OFFICE (2008) Data Handling Review. *Available at: http://www.cabinetoffice.gov.uk/newsroom/statements/080625_data_handling.aspx (Accessed: 7 June 2009).*

UK INFORMATION COMMISSIONER'S OFFICE (2007) Privacy Impact Assessment Handbook. *Available at: http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx (Accessed: 27 September 2008).*

UK INFORMATION COMMISSIONER'S OFFICE (2008a) Privacy by Design V2.0. *Available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf (Accessed: 6 June 2009).*

UK INFORMATION COMMISSIONER'S OFFICE (2008b) Taking stock, taking action, The ICO position on the Government Data, Handling Reviews. *Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico%20position%20paper%20on%20data%20loss%20reports.pdf (Accessed: 4 July 2009).*

UK INFORMATION COMMISSIONER'S OFFICE (2009) Privacy Impact Assessment Handbook V2.0. *Available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html (Accessed: 6 June 2009).*

US, Office of Management and Budget (2002) OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002. *Available at: http://www.whitehouse.gov/omb/memoranda/m03-22.html (Accessed: 25 March 2009).*

VAN DER LINDEN, H., KALRA, D., HASMAN, A. & TALMON, J. (2008) Inter-organizational future proof EHR systems: A review of the security and privacy related issues. IN INFORMATICS, I. J. O. M. (Ed.) *Available at: http://www.sciencedirect.com/science/article/B6T7S-4T9TC9S-2/2/c46d61e89cce64ba6c2c0fa67d769faf (Accessed: 23 November 2008).*

WIKIPEDIA (2009) Hippocratic Oath. *Available at: http://en.wikipedia.org/wiki/Hippocratic_Oath (Accessed: 23 May 2009).*

WORLD PRIVACY FORUM (2006) MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You. *Available at: http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (Accessed: 23 May 2009).*

WORLD WIDE WEB CONSORTIUM (2007) Platform for Privacy Preferences (P3P) Project. *Available at: http://www.w3.org/P3P/ (Accessed: 3 July 2009).*

APPENDIX A – EVALUATION FORM

This section contains the Evaluation Form used to assess the privacy impact assessment process and handbook.

1. Thank you for taking part in the Privacy Impact Assessment. The purpose of this questionnaire is to get your views on the process. Was it useful? In what way? How could the process be improved?

The Privacy Impact Assessment handbook lists several potential benefits of doing a PIA. In which ways do you think it benefited the project?

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Avoids costly system modifications after go-live	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree
Avoids privacy breaches and the resulting loss of confidence	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree
Builds trust and increases the acceptance of the initiative	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree
Avoids negative publicity	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree
Ensures compliance with legislation	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree
Develops a privacy aware culture within the organisation	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree
Promotes informed decision making	☐ Strongly Agree	☐ Agree	☐ Neutral	☐ Disagree	☐ Strongly Disagree

	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Explains how privacy risks have been balanced against other factors.	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree

Other (please specify)

2. What are your views on the PIA process?

	Yes	No	Don't Know
Did the process uncover privacy risks that might not have come to light?	Yes	No	Don't Know
Did the process help in identifying options to address those privacy risks?	Yes	No	Don't Know
Would you use this approach on future projects or on enhancements to this project?	Yes	No	Don't Know

Comments

*

3. Guidelines for PIAs emphasise the need for stakeholder consultation. Do you think all the necessary stakeholders were involved or consulted on the PIA process?

☐ Yes

☐ No

☐ Don't know

Comments

4. Would you make the PIA report available to the Office of the Data Protection Commissioner if it was conducting an audit or investigation of the section?

☐ Yes

☐ No

☐ Don't know

Comments

5. In some jurisdictions PIA reports or summaries are made publicly available to increase public confidence. Do you think it would be a good idea to make the report or summary publicly available?

☐ Yes

☐ No

☐ Don't know

Comments

6. What are your views on the PIA handbook?

	Yes	No	Don't Know
Did you find the handbook easy to follow?	☐ Yes	☐ No	☐ Don't Know

	Yes	No	Don't Know
Were you familiar with privacy principles before starting the PIA?	Yes	No	Don't Know
Did you find the background information to be of a suitable level?	Yes	No	Don't Know
Were the questions relevant to your project?	Yes	No	Don't Know

Have you any suggestions for the handbook, e.g. sections or questions to be added?

7. What parts of the handbook and approach did you find most useful?

Introduction to privacy concepts

Overview of PIA process

Checklists related to data protection and FOI principles

Other

8. Thank you for completing this evaluation. Have you any other comments on the process or the handbook?

APPENDIX B – PIA HANDBOOK

Privacy Impact Assessment Handbook

Muireann O'Dea

22 April 2009

Table of Contents

1 PRIVACY IMPACT ASSESSMENT HANDBOOK

1.1 OVERVIEW

A Privacy Impact Assessment (PIA) is a review of the risks to the privacy of individuals of a proposed initiative which is carried out at the design stage. A PIA looks at compliance with legislation (data protection, freedom of information, etc.) and also at wider ethical issues. It involves the project team and representatives from stakeholder groups. The purpose is to identify potential privacy risks and how these can be avoided or mitigated through modifications to the system and processes. It should balance the privacy risks against whatever benefits the initiative offers in the public interest.

Frameworks for carrying out privacy impact assessments have been developed in Canada, New Zealand, Hong Kong, Australia and the UK and they are mandatory for some types of project in the US and Canada.

The results of a privacy impact assessment is a report which documents the objectives of the project, the information flows for personal data, the risks identified and how these will be avoided or mitigated. The report should be considered to be a living document that is reviewed periodically as the project progresses. The report demonstrates that a comprehensive review of privacy has been undertaken and it can be made available to officials such as the Data Protection Commissioner or the general public, where appropriate.

1.2 WHY DO A PIA?

The main benefits of a Privacy Impact Assessment is that it identifies potential privacy impacts and the appropriate precautions and safeguards before a system or process has been put in place. It is generally cheaper and more effective to identify these issues early on in a project rather than later when significant investment has been made.

A PIA can benefit an organisation and the general public because it:

- Avoids of costly system modifications after go-live
- Avoids of privacy breaches and the resulting loss of confidence
- Builds trust and increases the acceptance of the initiative
- Avoids negative publicity
- Ensures compliance with legislation
- Develops a privacy aware culture with the organisation
- Promotes informed decision making
- Explains how privacy risks have been balanced against other factors.

1.3 WHAT IS PRIVACY?

Privacy has been defined as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations"[1]. It has several aspects:

Privacy of the person or "bodily privacy": This is concerned with an individual's right over their own body. The issues include compulsory immunisation, blood transfusion without consent, compulsory provision of bodily samples and compulsory sterilization.

Privacy of personal behaviour or **"media privacy":** This is concerned with an individual's behaviour in both public and private. The issues include political and religious activities and sexual practice.

Privacy of personal communications: This is concerned with the right of people to communicate with each other via various media without interception or surveillance.

Privacy of personal data: This is concerned with the ability to control the amount and use of personal data held by organisations about an individual. Personal data is any data that, on its own or in conjunction with other data, identifies an individual.

Privacy Impact Assessments are primarily concerned with communications and data privacy, which is sometimes called "**information privacy**". However they can look at all aspects of privacy that are likely to be of concern to the public.

The right to privacy is not an absolute right and it must be balanced against other rights, such as the rights of society in general.

1.4 WHEN TO DO A PIA

A project that involves the gathering of personal data about significant numbers of individuals is an obvious candidate for a privacy impact assessment. Any initiative that involves one or more of the following features is a likely candidate for a PIA:

- The collection, processing or use of personal data
- Identity management or the introduction of a new identifier, e.g. the introduction of a personal health identifier.
- Technology for identification and authentication e.g. identity cards, smart cards, biometrics, electronic signatures
- Location technology that can identify the location of a device, e.g. mobile phone
- A new use for an existing identifier, e.g. using a passport number to track movement in and out of the country.
- A new delivery channel for an existing service, e.g. making a service available online where it previously required a person to attend an office in person.
- The linking of multiple databases containing personal data or the sharing of data between multiple agencies, e.g. "joined-up government"
- Outsourcing of public services involving personal data

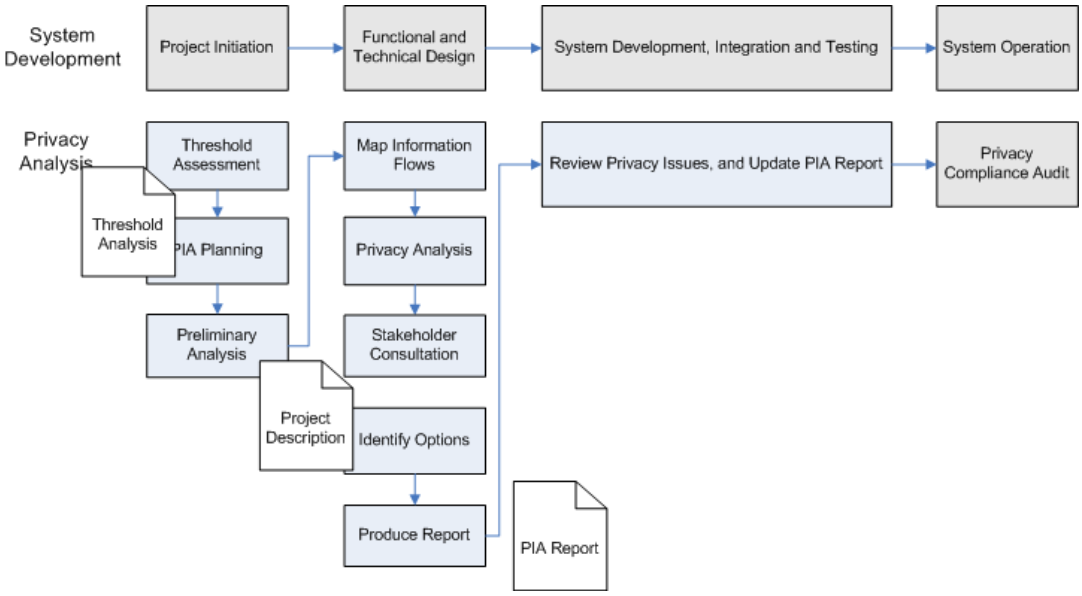
A privacy impact assessment is not required for all initiatives. For example, if no personal data is involved a PIA is not required.

Section 2 is a Threshold Assessment checklist that can be used to assess whether a PIA is required or not.

[1] Roger Clarke http://www.rogerclarke.com/DV/Privacy.html

1.5 OVERVIEW OF PROCESS

The following diagram shows how a privacy impact assessment fits in with the system development lifecycle:



During the initiation phase of the project a threshold assessment is carried out to determine if a PIA is warranted for the project.

If it is decided that a PIA is required the next stage is the plan the PIA. This includes identifying the people who will carry out the assessment and the main activities and timelines. Following on from this a preliminary privacy analysis is carried out. The aim of this is to describe at a high level the objectives of the project, the personal information that will be captured and how the project fits in with other initiatives.

The next phase is to map the business processes and information flows in detail. This happens in parallel with the functional and technical system design.

Next the business processes and information flows are analyses for potential privacy risks. The questionnaires provided in section 2 can be used to prompt the analysis. Depending on the size of the project, it may be appropriate at this stage to consult with internal and external stakeholders to get an understanding of any privacy concerns they may have.

The next stage is to analyse alternative designs and approaches to avoid or mitigate the privacy risks identified.

The final stage is to document the privacy analysis in the PIA Report. The privacy risks should be reviewed periodically as the system development proceeds, as changes to the system design may introduce new risks. The PIA report should be updated where appropriate.

Once the system is operational a privacy compliance audit may be carried out. This is not part of the privacy impact assessment, but the use of a PIA should ensure that the compliance issue have been considered in advance of the audit.

The main activities of the PIA are described in more detail below.

1.5.1 THRESHOLD ASSESSMENT

The purpose of the Threshold Assessment is to determine whether a PIA is required for the initiative. The checklist in section 1.6 can be used to guide this process.

The threshold assessment should be carried out by a senior member of the project team who understands the objectives and scope of the project and the person responsibility for privacy within the organisation. Depending on the scale of the project it may be necessary to consult with stakeholder groups to get their perspective on the project.

The results are documented in a short threshold analysis document. If it is decided that a PIA is not required then the PIA stops here and no further action is required. The threshold analysis document should be stored for future reference regardless of the outcome.

If it is unclear whether a PIA is required or not, it is recommended to complete the preliminary analysis and then make a reassessment. Alternatively the organisation could consult with the Office of the Data Protection Commissioner to get their advice.

1.5.2 PIA PLANNING

The PIA planning stage involves identifying the skills and resources required to carry out the PIA. The skills required will include

- Technical knowledge both for the proposed technical architecture and alternative technologies
- Risk and compliance skills
- Business process design
- Policy development skills
- Writing skills for the production of the PIA report
- Project management skills to manage the diverse inputs and ensure that tasks are completed
- Knowledge of information privacy principles and the legal framework.

Depending on the scale of the project the PIA could be carried out by one individual or by a team. Where the team lack certain skills it may be appropriate to include external consultants on the team. However the responsibility for the PIA should lie with the organisation, so that ownership lies with the organisation and privacy issues continue to be considered when the project has gone live.

The planning stage also needs to plan out the activities and the timescales for these. Where possible the PIA should be carried out early in the project lifecycle to identify risks early before there has been significant investment in system and process development.

The planning stage should also identify the terms of reference for the PIA and identify the individual within the organisation with responsibility for ensuring that the PIA is carried out effectively.

1.5.3 *Preliminary Analysis*

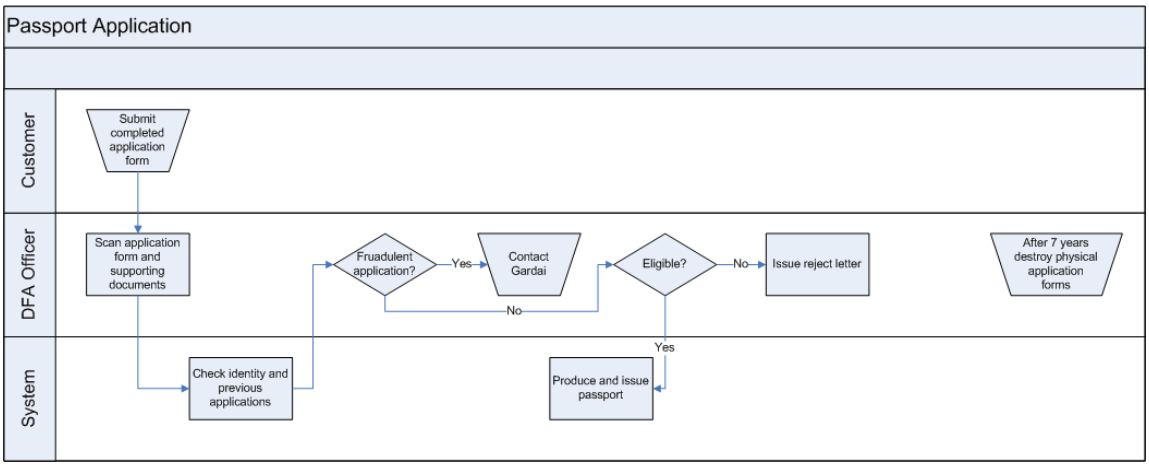
The aim of the preliminary analysis is to draft a high level overview of the project. The resulting report will include a description of:

- The project objectives and benefits
- The drivers or business rationale for the project
- The scope of the project
- Links with existing programmes
- An environmental analysis that looks at how similar objectives have been achieved in comparable organisations
- A stakeholder analysis that identifies the main stakeholder groups, i.e. the people or organisations that will be affected by the project, and their issues and concerns.
- A preliminary identification of privacy risks

The preliminary analysis sets the context for the subsequent phases of the PIA.

1.5.4 *Map Information Flows*

The purpose of this stage is to map the flow of personal data through the business processes. The first step is to map the business processes from an information management point of view. The business processes can be mapped out graphically using a flowchart notation such as the Business Process Modelling Notation (www.bpmn.org). The business process diagrams should show the activities, who or what is responsible for the activities and the flows of personal information. A sample business process diagram is shown below:



The following items need to be considered when mapping the information flows:

- The types of personal information that will be collected
- How the information is collected
- How the information is validated
- The intended uses of the information
- How the information is distributed and who will have access to it
- What transactional data is captured
- Whether the information is archived or destroyed after a period of time
- What security measures are in place, both procedural and technical
- What privacy legislation applies to the data flows

For complex systems there may be multiple business processes and information flows.

1.5.5 *Privacy Analysis*

The next stage is to analyse the information flows for compliance with data protection principles and with wider privacy and ethical standards. Section 3 contains a series of questions grouped by the eight data protection principles contained in legislation. Not all questions will apply to all projects, and conversely the environmental analysis in the preliminary phase may identify additional issues that have arisen in other jurisdictions that merit consideration.

The goal is to establish if the project will comply with data protection principles, to highlight any potential privacy risks and to anticipate public reaction.

Where privacy risks are identified these should be analysed to determine the likelihood of occurrence and the severity of the impact if they do occur. The privacy risks identified should be logged in an issues log.

1.5.6 *Stakeholder Analysis & Consultation*

Stakeholder consultation is important to identify privacy risks and to build awareness and confidence in the project. The stakeholders are those people and organisations directly involved in the project, those who will benefit from the project and others who may be affected by it. Stakeholder analysis starts during the Preliminary Phase of the PIA and is reviewed subsequent phases of the project. The following is a list of the potential stakeholders for a project:

- The organisation itself
- Participating organisations, e.g. sub-contractors, software suppliers
- Regulatory agencies
- Individuals as consumers, citizens, or employees
- The general public (where possible try to identify sub-groups)
- Advocacy groups

A stakeholder consultation plan should be developed as part of the overall PIA plan. The stakeholder s selected need to be representative of all the stakeholders. In some cases members of the organisation have sufficient understanding of the stakeholder groups to represent them. In cases where the general public are stakeholders consideration needs to be given as to whether they will be represented by advocacy groups, or whether selected members of the public will be asked to form focus groups. The consultation plan should allow for communication of details of the project to the stakeholders so that they are sufficiently well informed to contribute to the consultation process. The plan should also allow for multiple rounds of consultation as design options are reviewed and decisions taken.

The stakeholder consultation plan should be implemented in parallel or in conjunction with the privacy analysis phase. Any privacy risks or concerns identified during the stakeholder consultation should be added to the issues log.

1.5.7 *Identify Design Options*

The next stage is to identify and consider alternative business processes, procedures and system designs that could eliminate or mitigate the privacy risks identified. These options need to be considered in the light of the project goals so that the privacy risks can be balances against the planned benefits of the initiative.

The design options should be documented in the issues log, and when design decisions are taken to eliminate or mitigate privacy risks these decisions should also be included in the log.

1.5.8 PRODUCE REPORT

The final stage is the produce the PIA report. Typically the report will have the following sections:

Introduction

Scope of PIA

Participants

List of Applicable Legislation

Project Overview

Objectives

Project Description

Related Initiatives

Information Flows

Privacy Analysis

Responses to DPP Checklists

Privacy Risk Assessment and Options

Communications Strategy

Conclusions & Recommendations

The report is a useful resource which can be used to explain the project to senior management, privacy auditors and the data protection commission. In many jurisdictions these reports are made available to the public so as to increase confidence in the initiative.

The report can be used in subsequent phases of the project when extensions or changes to the process are under consideration. It can also be used as a guide for similar projects.

2 THRESHOLD ASSESSMENT CHECKLIST

Project/Program Name: **Project/Program Contact:** **Title:** **Date Completed:**		
A Privacy Impact Assessment (PIA) is advisable where an initiative is likely to result in a substantive change to the collection, use, disclosure or retention of personal data. A "Yes" answer to any of the questions below indicates that a PIA is advisable.		
Category	**Response**	**Notes**
Personal Data		
1. Does the project involve collection use or disclosure of personal data? Personal information means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information. Certain categories of individuals may be easier to identify, e.g. minority groups.	☐ Yes ☐ No	
2. Does the project involve a new use for personal information already held? Where data collected for one purpose is to be use for another purpose the consent of the individuals may be required.	☐ Yes ☐ No	
3. Does the project involve the collection, use or disclosure of sensitive personal data such as health data? The Data Protection Act defines certain categories of "sensitive personal data" which includes data related to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.	☐ Yes ☐ No	
4. Does the project involve the use of personal data for research or statistics, whether de-identified or not?	☐ Yes	

The use of data for research raises the issue of consent, and the process of de-identifying data may need to be verified.	☐ No	
Data Handling		
5. Does the project involve new or significantly changed handling of a considerable amount of personal data about each individual in the database? Examples include intensive data processing such as welfare administration, healthcare, consumer credit, and consumer marketing based on intensive profiles.	☐ Yes ☐ No	
6. Does the project involve the consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources? Issues arise in relation to data quality, the diverse meanings of superficially similar data-items, and the retention of data beyond the very short term.	☐ Yes ☐ No	
Technology		
7. Does the project involve the use of technology that has the potential to be privacy intrusive? Examples include: smart cards, radio frequency identification (RFID) tags, biometrics, locator technologies (including mobile phone location, applications of global positioning systems (GPS) and intelligent transportation systems), visual surveillance, digital image and video recording, profiling, data mining, data warehousing and logging of electronic traffic.	☐ Yes ☐ No	
Identity		
8. Does the project involve the use of new or existing personal identifiers and identity management? Examples include digital signatures, smart cards, RFID tags, multi-purpose identifiers and biometrics. Schemes of this nature have considerable potential for privacy impact and give rise to substantial public concern and hence project risk.	☐ Yes ☐ No	

9. Does the project covert previously anonymous transactions into identified transactions? For example, if services are to be provided on the Internet, does someone have to identify themselves to access these services, where previously they could have got the information anonymously, e.g. by a telephone enquiry.	☐ Yes ☐ No	
Multiple Organisations		
10. Does the project involve linking of data from multiple organisations (either private or public-sector)? Examples include "joined-up government initiatives or outsourcing to private sector organisations. Compensatory protection measures may need to be considered.	☐ Yes ☐ No	
Exemptions		
11. Does the project relate to data processing which is in any way exempt from legislative privacy protections? Examples include law enforcement and national security information systems and also other schemes where some or all of the privacy protections have been negated by legislative exemptions or exceptions.	☐ Yes ☐ No	
General		
12. Does the proposal contain any other measures that may affect privacy or that would raise privacy concerns with the public? It is important to consider the perspectives of all stakeholders of the project, not just the agency involved. Areas to be considered include surveillance, privacy of communication, bodily privacy, etc.	☐ Yes ☐ No	

3 COMPLIANCE CHECKLISTS

This section contains a series of checklists for each of the principles contained in the data protection act and freedom of information act. These are intended to act as prompts for discussion. A no answer to any question indicates that privacy issues have may not have been fully addressed.

DPP1. Obtain and process information fairly

Background

To fairly obtain data the data subject must, at the time the personal data is being collected, be made aware of organisation collecting the data, the purpose of collecting the data and how that data will be processed.

The data subject must have given consent to the processing or the processing must be necessary to comply with a legal obligation, to prevent damage to the health of the data subject, or serious loss to the property of the data subject.

There are additional special conditions in relation to sensitive personal data:

The data subject has given explicit consent (or where they are unable to do so, for reasons of incapacity of age, explicit consent must be given by a parent or legal guardian) to the processing, OR

The processing must be necessary for one of the following reasons -

- for the purpose of exercising rights or obligations conferred by law on the data controller in connection with employment;
- to prevent damage to the health of the data subject or another person, or damage to property or otherwise to protect the vital interests of the data subject or of another person in a case where, consent cannot be given;
- to prevent damage to the health of another person, or damage to the property of another person, where such consent has been unreasonably withheld;
- it is carried out by a not for profit organisation in respect of its members;
- the information being processed has been made public as a result of steps deliberately taken by the data subject;
- for the purpose of obtaining legal advice, or defending legal rights;
- for medical purposes;
- it is carried out by political parties or candidates in the context of an election;
- for the purpose of the assessment or payment of a tax liability;

- in relation to the administration of a Social Welfare scheme.

Patient Consent To Collecting Information

The consent of the patient should, where possible, be obtained when obtaining personal health information. Accordingly, at the time of collecting personal health information, healthcare professionals and health agencies must take reasonable steps to ensure that the patient understands:

- what information is being collected;
- why the information is being collected;
- who within the practice will have access to the information;
- how the information will be used including, where applicable, that it may be used for research purposes;
- where relevant, the fact that there is a statutory obligation to collect the information (e.g. disease notification requirements);
- any proposed disclosure of the information to third parties;
- that the patient can have access to the information, once collected;
- the consequences of not providing the information;
- if relevant, that the information will be computerised; and
- where the information is being collected by the healthcare professional on behalf of an organisation (e.g. the HSE), the identity of the organisation and how to contact it.

The information must be necessary for the purpose for which it is collected, and must be collected in a way that is lawful, fair and not unreasonably intrusive.

Wherever it is reasonable and practicable to do so, personal health information about a patient must be collected directly from the patient rather than from third parties.

Discussion

Question	Yes	No	N/A	Notes
At the time of data collection is the client aware of the: • The data being collected • The primary purpose of the data collection • The authority under which it is collected • The identity of the data controller				
Is consent sought at the time of data collection for any **secondary purposes** for the data collection, including research?				
Can the client opt-out of secondary purposes, while still availing of the primary purpose?				
Is the client consent, or otherwise, to the primary and secondary purposes recorded and dated?				
If the data may be **disclosed to third parties** is the client made aware of this at the time of data collection?				
Where possible, is the data obtained directly from the client?				
If the data is **obtained through a third party** is the client made aware of the data collection and the purpose of this?				
Does the client give explicit **consent** to capture the data and, if not, is there a legitimate reason for collecting the data?				
If the project involves the collection of **sensitive personal data** is the client asked for explicit consent and, if not, is there a legitimate reason for collecting the data?				
Could the data-collection practices be described as open, transparent and up-front?				

DPP2. Keep it only for one or more specified, explicit and lawful purposes

Background

You may only keep data for a purpose(s) that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with that purpose(s). An individual has a right to question the purpose for which you hold his/her data and you must be able to identify that purpose.

To comply with this rule:

- In general a person should know the reason/s why you are collecting and retaining their data.
- The purpose for which the data is being collected should be a lawful one
- You should be aware of the different sets of data which you keep and specific purpose of each

Discussion

Question	Yes	No	N/A	Notes
Has a clear relationship been identified between the data to be collected and the purpose of the data collection?				
Has responsibility been assigned for maintaining a list of all data sets and the purpose associated with each?				
Does the application form clearly identify the purposes for which the data is collected, the legal authority for collection and the contact details for enquiries about the purpose?				
Is this information available through all application channels (web, phone, kiosk, etc)?				
Is client consent sought for secondary purposes, e.g. service quality monitoring?				
Are the secondary purposes are not identified on the application form clearly identified elsewhere?				
If you are required to register with the Data Protection Commissioner, does the register entry include a proper, comprehensive statement of your purpose(s)?				

DPP3. Use and disclose it only in ways compatible with these purposes

Background

Any use or disclosure must be necessary for the purpose(s) or compatible with the purpose(s) for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use of or disclosure of their data is taking place.

A key test of compatibility is:

- Do you use the data only in ways consistent with the purpose(s) for which they are kept?
- Do you disclose the data only in ways consistent with that purpose(s)?

The rule, that disclosures of information must always be compatible with the purpose(s) for which that information is kept, is lifted in certain restricted cases by Section 8 of the Data Protection Act. Examples of such cases would include some obvious situations where disclosure of the information is required by law or is made to the individual himself/herself or with his/her consent.

Using, Disclosing and Transferring Personal Health Information

Subject to exceptions provided by law, personal health information held by medical practitioners can only be used or disclosed:

• for the purpose for which it was collected; or

• for another directly-related purpose that is within the reasonable expectations of the patient at the time he or she provided the information.

Personal health information can be used or disclosed to others for some other purpose if:

• the patient concerned has consented to the use or disclosure; or

• the medical practitioner reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health or public safety; or

• the use or disclosure is required or authorised by law (e.g. statutory duties to notify certain infectious diseases or suspected child abuse, or compliance with a subpoena or court order); or

• the information concerns a patient who is incapable of giving consent, and is disclosed to a person responsible for the patient to enable appropriate care or treatment to be provided to the patient.

Any disclosure should be limited to that which is either authorised or required in order to achieve the desired objective.
Personal health information can be transferred to an individual or organisation outside the European Economic Area only if:

• the patient has given consent for the transfer; or

• it is impracticable to obtain patient consent, but the proposed transfer of information is for the benefit of the patient and the patient would be likely to give consent, if asked.

The general principle governing the use, disclosure or transfer of all personal health information is that the patient must understand what the healthcare professional proposes to do with the information and must agree with this proposed use. Only in certain very limited circumstances is it lawful to use, disclose or transfer personal health information without the consent of the patient.

Discussion

Question	Yes	No	N/A	Notes
Are there defined rules about the use and disclosure of information?				
Are all staff aware of these rules?				
Are the individuals aware of the uses and disclosures of their personal data? Would they be surprised if they learned about them?				
If you are required to register with the Data Protection Commissioner, does the register entry include a full list of persons to whom you may need to disclose personal data?				
Are personal identifiers such as the PPS Number used to link data across multiple databases?				
Where data matching or profiling occurs is it consistent with the stated purposes for which the data was collected?				

DPP4. Keep it safe and secure

Background

Appropriate security measures must be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. The security of personal information is all-important, but the key word here is appropriate, in that it is more significant in some situations than in others, depending on such matters as confidentiality and sensitivity and the harm that might result from an unauthorised disclosure. High standards of security are, nevertheless, essential for all personal information. The nature of security used may take into account what is available technologically, the cost of implementation and the sensitivity of the data in question.

A minimum standard of security would include the following:

- access to central IT servers to be restricted in a secure location to a limited number of staff with appropriate procedures for the accompaniment of any non-authorised staff or contractors;
- access to any personal data within an organisation to be restricted to authorised staff on a 'need-to-know' basis in accordance with a defined policy;
- access to computer systems should be password protected with other factors of authentication as appropriate to the sensitivity of the information;
- information on computer screens and manual files to be kept hidden from callers to your offices;
- back-up procedure in operation for computer held data, including off-site back-up;
- all reasonable measures to be taken to ensure that staff are made aware of the organisation's security measures, and comply with them;
- all waste papers, printouts, etc. to be disposed of carefully;
- a designated person should be responsible for security and for periodic reviews of the measures and practices in place.

Discussion

Question	Yes	No	N/A	Notes
Are there documented security provisions in place for each data set?				
Is someone responsible for the development and review of these provisions?				
Are these provisions appropriate to the sensitivity of the personal data?				
Are the computers and our databases password-protected, and encrypted if appropriate?				
Are the computers, servers, and files securely locked away from				

unauthorised people?				
Are there measures in place to secure against unauthorised access to personal data?				
Have staff been trained in the security policies and are they aware of policies regarding breaches of security?				
Is read access to personal data audited by date and user?				
Are changes to personal data audited by date and user?				
Are there procedures in place to review audit trails to check for unauthorised access?				
Are access rights only provided to users who require access for stated purposes?				
Is user access to personal data limited to that required for the stated purposes?				
Are there procedures in place to notify security violations to stakeholders and data subjects?				
Are there procedures in place to notify security violations to the appropriate ministers and law enforcement agencies?				
Are there procedures in place to guard against leaving medical notes unattended at a public counter?				
Are there procedures in place for securely disposing of health records?				
Are there procedures in place to guard against sensitive data being held on laptops which may be taken off-site?				

DPP5. (FOI) Keep it accurate, complete and up-to-date

Background

Apart from ensuring compliance with the Acts, this requirement has an additional importance in that you may be liable to an individual for damages if you fail to observe the duty of care provision in the Act applying to the handling of personal data which tends to arise substantially in relation to decisions or actions based on inaccurate data. In addition, it is also in the interests of your business to ensure accurate data for reasons of efficiency and effective decision making.

To comply with this rule you should ensure that:

- Your clerical and computer procedures are adequate with appropriate cross-checking to ensure high levels of data accuracy (apart from back-up data);
- The general requirement to keep personal data up-to-date has been fully examined;
- Appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.

Discussion

Question	Yes	No	N/A	Notes
Is the data checked for accuracy?				
Do we know how much of the personal data is time-sensitive, i.e. likely to become inaccurate over time unless it is updated?				
Are steps taken to ensure your databases are kept up-to-date?				
Is a record of the last update date kept?				
Is there a procedure to allow an individual to request corrections to their data?				
Where appropriate is there a way of notifying third parties where data was updated that was previously supplied to them?				
Is the health information organised in a way that minimises the potential for the personal health information of one individual being confused with another?				

DPP6. Ensure that it is adequate, relevant and not excessive

Background

You can fulfil this requirement by making sure you are seeking and retaining only the minimum amount of personal data which you need to achieve your purpose(s). You should decide on specific criteria by which to assess what is adequate, relevant, and not excessive and apply those criteria to each information item and the purpose/s for which it is held.

To comply with this rule you should ensure that the information sought and held is:

- Adequate in relation to the purpose/s for which you sought it;
- Relevant in relation to the purpose/s for which you sought it;
- Not excessive in relation to the purpose/s for which you sought it.

A periodic review should be carried out of the relevance of the personal data sought from data subjects through the various channels by which information is collected, i.e. forms, website etc. In addition, a review should also be undertaken on the above basis of any personal information already held.

Adequate health information should include: symptoms voiced by the patient; tests undertaken; facts, analysis and opinions presented to the patient; correspondence from the patient or other parties; the identification of problems that have arisen and the action taken to rectify them, evidence of the care planned, decisions made, care delivered and information shared.

Discussion

Question	Yes	No	N/A	Notes
Does the data collection include all the information needed to serve the specified purpose effectively, and to deal with individuals in a fair and comprehensive manner?				
Have you checked to make sure that all the information you collect is relevant, and not excessive, for your specified purpose?				
Have ways to limit the amount of data collected been explored?				
Can you justify every piece of information held about an individual, if requested to do so by an individual?				
Does a policy exist in this regard?				
Is the health information devoid of irrelevant, prejudicial, derogatory, malicious, vexatious information or comment?				
Is the health information comprehensible and legible, which may be important if it is to be used in an emergency?				

DPP7. Retain it for no longer than is necessary for the purpose or purposes

Background

Data controllers should be clear about the length of time for which data will be kept and the reason why the information is being retained. Personal data collected for one purpose cannot be retained once that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Acts attach to it. If you don't hold it anymore then the Acts don't apply.

To comply with this rule you should have:

- A defined policy on retention periods for all items of personal data kept;
- Management, clerical and computer procedures in place to implement such a policy.

It is accepted medical practice that individual patient medical records be retained for a *minimum* of eight years from the date of last contact or for any period prescribed by law. (In the case of children's records, the period of eight years generally begins from the time they reach the age of majority). In other cases, healthcare professionals or agencies holding personal health information may decide that it is in the patient's, and their own, best interests that it should be retained indefinitely.

Discussion

Question	Yes	No	N/A	Notes
Is there a clear statement on how long items of information are to be retained?				
Are you clear about any legal requirements to retain data for a certain period?				
Do you regularly purge our databases of data which we no longer need, such as data relating to former customers or staff members?				
Do you have a policy on deleting personal data as soon as the purpose for which it was obtained has been completed?				

DPP8. (FOI) Give a copy of his/her personal data to an individual, on request

Background

On making an access request any individual about whom you keep personal data is entitled to:

- a copy of the data you are keeping about him or her;
- know the categories of their data and your purpose/s for processing it;
- know the identity of those to whom you disclose the data;
- know the source of the data, unless it is contrary to public interest;
- know the logic involved in automated decisions;
- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given.

It is important that you have clear co-ordinated procedures in place to ensure that all relevant manual files and computers are checked for the data in respect of which the access request is being made.

- Access to Health and Social Work Data

There are modifications to the right of access in the interest of the data subject or the public interest, designed to protect the individual from hearing anything about himself or herself which might cause serious harm to his or her physical or mental health or emotional well-being;

Patient Access to Personal Health Information

An individual, or person acting on his or her behalf, should have a right of access to any personal health information concerning him or her and be entitled to have that information enhanced, corrected, blocked or otherwise amended (including by deletion where this is not inconsistent with the keeping of a proper healthcare record) to bring it into line with any or all of the above principles.
The general rule is that patients have a right to have access to their personal health information irrespective of the form in which it is kept.

Where a patient requests an alteration or correction to their personal health information, healthcare professionals should note details of the request on the medical record and indicate whether they agree that the request for alteration or correction is appropriate.
Healthcare professional can refuse patients access to their personal health information only if:

- providing access would pose a serious threat to the life or health of any individual, including the requestor;
- providing access would have an unreasonable impact on the privacy of other individuals;
- denying access is required or authorised by law.

A healthcare professional should forward, on request, a full copy of the records of a patient to another healthcare professional where the patient so requests and should make similar arrangements to forward such information where he or she intends to retire or resign from practice.

Discussion

Question	Yes	No	N/A	Notes
Is a named individual responsible for handling access requests?				
Are there clear procedures in place for dealing with such requests?				
Do these procedures guarantee compliance with the FOI Act's requirements?				
Has the system been designed so that all the personal data for a data subject can be provided easily?				

FOI 1 Openness

The Freedom of Information Act establishes three statutory rights:

- The right to access records held by public bodies
- The right to have personal information in a record amended where it is incomplete, incorrect or misleading
- The right to obtain reasons for decisions affecting the person.

Question	Yes	No	N/A	Notes
Is the stated purpose of the initiative covered by the FOI legislation?				
Does the organisation provide accessible information on the rules and procedures used in decision making?				
Does an individual have access to the reason why a decision was made in relation to them?				

Registration and Compliance

Question	Yes	No	N/A	Notes
Are you clear about whether or not you need to be registered with the Data Protection Commissioner?				
If registration is required, is the registration kept up to date?				
Is a named individual responsible for meeting the registration requirements?				
Has a data protection co-ordinator and compliance person been appointed?				
Are all staff aware of their role?				
Are there mechanisms in place for formal review by the co-ordinator of data protection activities within our organisation?				

Training

Question	Yes	No	N/A	Notes
Do you know about the levels of awareness of data protection in the organisation?				
Are staff aware of their data protection responsibilities - including the need for confidentiality and the sensitive nature of health information?				
Is data protection included in the training programme for staff?				

4 GLOSSARY

Data means information in a form which can be processed. It includes both automated data and manual data.

Automated data means any information held electronically.

Manual data means information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Relevant filing system means any set of information that, while not computerised, is structured by reference to individuals, or by reference to criteria relating to individuals, so that specific information is accessible.

Personal data means data relating to a living 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. This can be a very wide definition depending on the circumstances.

Processing means performing any operation or set of operations on data, including:

- Obtaining, recording or keeping data,
- Collecting, organising, storing, altering or adapting the data,
- Retrieving, consulting or using the data,
- Disclosing the information or data by transmitting, disseminating or otherwise making it available,
- Aligning, combining, blocking, erasing or destroying the data.

Data Subject is an individual who is the subject of personal data.

Data Controllers are those who, either alone or with others, control the contents and use of personal data. Data Controllers can be either legal entities such as companies, Government Departments or voluntary organisations, or they can be individuals such as G.P.'s, pharmacists or sole traders.

Data Processor is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment. Again individuals such as GPs, pharmacists or sole traders are considered to be legal entities.

Sensitive personal data relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs; physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

5 RESOURCES

Office of the Data Protection Commissioner Website:
www.dataprotection.ie

Freedom of Information Website:
www.foi.gov.ie

UK Privacy Impact Assessment Handbook:
http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

Australian Privacy Impact Assessment Handbook:
http://www.privacy.gov.au/publications/pia06/index.html

US Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
http://www.whitehouse.gov/omb/memoranda/m03-22.html

Ontario Privacy Impact Assessment Handbook:
http://www.accessandprivacy.gov.on.ca/english/pia/pia1.pdf

New Zealand Privacy Impact Assessment Handbook:
http://www.privacy.org.nz/filestore/docfiles/48638065.pdf