Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

International Review of Secondary Use of Personal Health Information

January 2012

Safer Better Care

About the Health Information and Quality Authority

The Health Information and Quality Authority is the independent Authority which was established under the Health Act 2007 to drive continuous improvement in Ireland's health and social care services. The Authority was established as part of the Government's overall Health Service Reform Programme.

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

Setting Standards for Health and Social Services – Developing person-centred standards, based on evidence and best international practice, for health and social care services in Ireland (except mental health services)

Monitoring Healthcare Quality – Monitoring standards of quality and safety in our health services and implementing continuous quality assurance programmes to promote improvements in quality and safety standards in health. As deemed necessary, undertaking investigations into suspected serious service failure in healthcare

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

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

Social Services Inspectorate – Registration and inspection of residential homes for children, older people and people with disabilities. Monitoring day- and pre-school facilities and children's detention centres; inspecting foster care services.

Overview of Health Information function

Health is information-intensive, generating huge volumes of data every day. It is estimated that up to 30% of the total health budget may be spent one way or another on handling information, collecting it, looking for it, storing it. It is therefore imperative that information is managed in the most effective way possible in order to ensure a high quality, safe service.

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

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

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

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

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

Information can be lost, documentation is poor, and there is over-reliance on memory. Equally those responsible for planning our services experience great difficulty in bringing together information in order to make informed decisions. Variability in practice leads to variability in outcomes and cost of care. Furthermore, we are all being encouraged to take more responsibility for our own health and well-being, yet it can be very difficult to find consistent, understandable and trustworthy information on which to base our decisions.

As a result of these deficiencies, there is a clear and pressing need to develop a coherent and integrated approach to health information, based on standards and international best practice. A robust health information environment will allow all stakeholders – patients and service users, health professionals, policy makers and the general public to make choices or decisions based on the best available information. This is a fundamental requirement for a highly reliable healthcare system.

Through its health information function, the Authority is addressing these issues and working to ensure that high quality health and social care information is available to support the delivery, planning and monitoring of services. One of the areas currently being addressed through this work programme is the need to develop a framework for information governance in Ireland. This international review is the first step in exploring best practice in the secondary use of information and how it is managed, which is part of the information governance framework development programme.

Table of Contents

Executive Summary

The need for an information governance (IG) framework was identified in the 2004 *National Health Information Strategy*[1] (NHIS) which stated that a specialist function for IG would be established by the Health Information and Quality Authority (the Authority).

One of the aims of the forthcoming Health Information Bill is to put health IG on a sound and robust footing within the Irish health and social care sector. The primary mandate of the Authority is to drive patient safety in health and social care in Ireland. In relation to health information, this also includes ensuring that service users' interests are appropriately protected. This includes the right to privacy, confidentiality and security of their personal health information. It is anticipated that the Health Information Bill will include explicit provisions governing the secondary use of personal health information.

In line with the NHIS, the provisions in the Draft Heads of Health Information Bill[2] and the Authority's remit to develop standards, the Authority has commenced work on developing an IG framework for the Irish health and social care sector.

Information governance (IG) refers to a strategic framework that brings coherence and transparency to information initiatives and which is responsive to the spectrum of issues and concerns of those involved. Issues such as information sharing, health surveillance, quality assurance, confidentiality, privacy, records management, freedom of information and data protection are all included[1].

Good IG is essential in ensuring an appropriate balance between using personal health information as required to provide appropriate and safe care, and protecting the rights and interests of service users. With so much information being collected, used and shared in the provision of health and social care services, it is important that steps are taken to protect the privacy of each individual and ensure that sensitive personal health information is handled legally, securely, efficiently and effectively in order to deliver the best possible care[3]. The appropriate secondary use of personal health information is a core component of this.

The term 'personal health information' is broad and includes such matters as personal information relating to the physical or mental health of the individual, as well as any genetic data or human tissue data that could be predictive of the health of the individual or his/her relatives or descendants. In essence, it covers any information relating to an individual that is collected for, or in connection with, the provision of a health service[3].

The Authority is concerned with the secondary use of personal health information in the context of IG and, as such, the term 'secondary use of information' should, throughout this document, be interpreted to mean the secondary use of personal health information. The secondary use of information means using the information for any purpose other than that for which it was originally collected. In the context of this report, this means other than for the provision of healthcare.

The secondary use of information can yield significant benefits for and improvements in service delivery and research. Using personal health information for secondary purposes, such as service planning, leads to better-informed decision-making leading to improvements in the efficiency and effectiveness of services.

However, this requires for service users to be comfortable with the use of their information. They need to be confident that their rights are being appropriately protected and respected and ultimately, that they are in control of how their information is being used.

The Authority has developed *National Standards for Safer Better Healthcare*, which at the time of writing this report are pending Ministerial approval. One of the standards requires service providers to have effective arrangements in place for IG. The purpose of this international review is to identify key themes around the secondary use of information to inform the development of detailed IG guidance that will assist service providers in improving IG practices and meeting the requirements in the *National Standards for Safer Better Healthcare*.

International Review

An initial desktop review of the secondary use of personal health information, and its key principles in health and social care, identified four countries for further examination. The countries were chosen based on secondary use initiatives, resources identified in the desktop review, and the availability of information. The review examines the following countries:

- England
- Canada
- New Zealand
- Australia.

A brief overview of the current legislation and guidance available on secondary use of information in Ireland is also given in the introductory section of the document.

Findings

Of the information that was sourced in the course of this review the following are the key points:

Increased need for guidance on the secondary use of information:

One of the findings of the review was that there is a consensus regarding the need for guidance around the secondary use of information. Legislative provisions concerning the secondary use of information are typically contained within general privacy or data protection legislation.

Guidance and codes of practice have typically centred on privacy and confidentiality with the appropriate secondary use of information being covered as an aspect within it. More recently, guidance is emerging that focuses solely on how information can be used and disclosed – focusing in particular on what secondary uses are appropriate.

Examples include the British Medical Association's document *How to respond to requests for disclosure of data for secondary purposes*[4], the College of Physicians and Surgeons of Alberta's *Framework for the secondary use of health information*[5] and in Australia the *Handbook for the Management of Health Information in Private Medical Practice*[6].

Informing and involving service users in decision about personal health information:

The key recommendation in the guidance documents explored as part of this review was the need to be open and transparent with service users about the various uses to which their information is put. The importance of informing and engaging with service users about how their information may be used is reiterated in guidance documents and codes of practice that were sourced in each of the countries explored.

A number of the guidance documents emphasise the ways in which this can be done. For example, posters and leaflets in waiting rooms outlining the ways in which information may be used and the reasons for it. One example as documented in the Australian *Handbook for the Management of Health Information in Private Medical Practice*[6] is the use of information for quality assurance purposes.

Patients should be made aware that their information may be used for this purpose and have the benefits of the practice clearly explained to them. A recurring message can be identified in the literature which asks health professionals if a patient would be surprised to learn that their information was being used in this way – if so they are not being effectively informed.

Differentiation between types of secondary use:

One of the findings in the course of the review is that clear distinctions are drawn between different secondary uses of health information, for example use for teaching purposes, quality assurance purposes (such as clinical audit), and research purposes.

However, the categorisation of clinical audit in itself is not clearly defined - for example, in England it is seen to be a primary healthcare function where the audit is carried out internally by the NHS organisation, but if it requires disclosure to an external auditor it is classed as a secondary use of the information.

In the guidance explored, different steps are outlined which must be followed depending on the type of use. The *NHS Code of Practice on Confidentiality*[7] presents a model outlining three different types of disclosure – for healthcare purposes (which includes clinical audit when conducted internally), medical purposes other than healthcare (for example, disclosure to cancer registries), and non-medical purposes (for example, to a hospital chaplain).

The National Ethics Advisory Committee in New Zealand has produced ethical guidelines for observational research[8] which base their requirements for ethical review on the principle that the intensity of ethical scrutiny should be proportionate to the level of risk of the activity.

Consent:

The review identified consent as a key concept to be addressed in the context of the secondary use of health information. At the most basic level of interpretation, consent must be obtained for the collection, use or disclosure of information for purposes outside the direct provision of care.

However, there are caveats to this - based on the type of secondary use as outlined above, whether consent needs to be explicit or whether implied consent will suffice (for example, by informing patients that their information may be used for local clinical audit through leaflets or posters in a waiting room) and steps that can be taken where it is not possible to gain consent.

The conditions that must be satisfied vary between countries depending on legislative requirements. In some cases, bodies have been established to specifically provide guidance and advice in this area for example, the Ethics and Confidentiality Committee in England. The approval of research ethics committees and their requirements are also central to the ability to proceed without the consent of the individuals concerned. Despite the variations between rules and provisions internationally the optimum position in all cases is to obtain consent.

Anonymisation:

One of the findings of the review is the recommendation that, where possible, information should be anonymised before it is used for secondary purposes.

In Ireland, once information has been anonymised the provisions of the Data Protection Acts cease to apply as the information is no longer identifiable. The legislative provisions are similar internationally, but questions have been raised around the definition of the term anonymised. For example, can information be said to be anonymised if the process is reversible?

Irrevocable anonymisation of personal data puts it outside data protection requirements in Ireland as it can no longer be linked to an individual. Guidance recommends that for all secondary uses, information should be anonymised at the earliest point possible in the process. Typically, where anonymised information is being used, consent is not required but best practice suggests that patients should still be informed.

Data Sharing Agreements:

One of the findings of the review is that data sharing agreements offer an additional safeguard against inappropriate use of information once it has been disclosed to a person or body outside the organisation (data controller).

Typically, they require the body receiving the information to adhere to the same principles that the data controller does in respecting the privacy, confidentiality and security of the information.

The IG toolkit in the UK requires that secondary use organisations agree protocols governing the routine sharing of personal information with other organisations. Legislation within Canadian provinces is increasingly dictating the need for the Canadian Institute for Health Information (CIHI) to enter into data sharing agreements with third party data recipients. CIHI also undertakes audits of third party data recipients to ensure that they meet their contractual obligations.

Next Steps

Using the information sourced in this review, the next step in the Authority's programme of work will be to identify the themes and principles that can be appropriately tailored to the Irish health and social care sector.

This will inform the development of detailed IG guidance, which will assist providers in complying with the forthcoming *National Standards for Safer Better Healthcare* which includes a requirement for service providers to have effective arrangements in place for IG.

The detailed IG guidance will also act as a general resource for all health and social care professionals.

1. Introduction

1.1 Background and overview

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

The *National Health Information Strategy 2004* calls for the development of a framework for IG[1]. The strategy states, within this action, that a specialist function for IG will be established by the Authority.

In line with this, and the provisions in the Health Act 2007, the development of such a framework has been identified as a priority for the Authority. This work will be completed in line with the provisions of the Health Information Bill and informed by consultation with key, relevant, stakeholders. It is anticipated that the provisions of the Health Information Bill will include legislative provision for the development of IG standards.

The Authority is currently working towards developing a framework/structure for IG for the Irish health and social care sector. As a first step in this process the Authority undertook an *International Review of Information Governance Structures*[9] and an *As Is Analysis of Information Governance in Health and Social Care Settings in Ireland*[10]. In the course of these reports the following topics were identified as the core aspects of IG:

- IG management
- information security
- data quality
- privacy and confidentiality
- secondary use of information.

The components of each of these aspects, when developed and implemented in an organisation, comprise an IG framework. Each of these is also covered at a high level in the *National Standards for Safer Better Healthcare* developed by the Authority.

Under these Standards, service providers will be required to have effective arrangements in place for IG. At the time of writing this report the *National Standards for Safer Better Healthcare* are pending ministerial approval. The National Standards have been designed to describe the principles of how healthcare should be provided in any setting.

In the future, the Authority will monitor compliance with these National Standards but they have also been developed as a resource for service users to help them understand what they should expect from a well-run service and what high quality and safe healthcare should be.

The purpose of this document is to inform the development of detailed IG guidance, which will assist providers in complying with the national standards and also act as a general resource for all health and social care professionals.

Personal health information includes all identifiable information relating to the physical and/or mental health of the individual. It covers any information relating to an individual that is collected for or in connection with the provision of a health service. It can be identifiable by a name, a date of birth, an address, an assigned number) such as a medical record number) or any other code that has been assigned to code the information.

Personal health information ceases to be 'personal' only when it has been anonymised to the point that it can no longer be linked to any known individual meaning the removal of all possible identifiers and ensuring that any other data or combination of data could not identify the individual.

Once this has been done, the provisions of the Data Protection Acts no longer apply. The Authority is concerned with ensuring that the appropriate safeguards are in place to protect service users' rights to privacy and confidentiality of their personal health information. As such in the context of this document the term secondary use of information can be taken to mean the secondary use of personal health information.

1.2 What is secondary use of information?

As a general rule, information should only be used for the purpose for which it was collected - that is, the primary purpose. Primary purpose relates to information which has been collected and is being kept by a custodian for the purpose of protecting, promoting, maintaining or meeting the physical and mental health needs of an individual[(2)].

Secondary use of information relates to information collected in the course of providing care, being used for purposes other than direct patient care. Service user data can be used for many valuable secondary purposes aside from research, which bring benefits to the patient population as a whole. Secondary uses include using information for audit and quality assurance purposes, performance monitoring, service planning and epidemiology[*].

The following table provides examples of how information is used for secondary purposes in Ireland:

Secondary Use	**Example**
Audit and quality assurance purposes	Use of patient healthcare records to complete clinical audits in hospitals to support continuous improvement in the delivery of care.
Performance monitoring	HealthStat is a performance information and improvement system designed and implemented by the Health Service Executive (HSE). It is a databank of performance information for Irish public health services. It allows the HSE to measure, for example, waiting times for services in public hospitals throughout the country, assess if targets are being met and identify areas where improvements are required.
Service planning	Hospital In-Patient Enquiry (HIPE)[†] data are used by the Department of Health and the HSE in the planning, provision and measurement of acute hospital services.

[*] Epidemiology is the study of the distribution and determinants of health-related states and events and the application of this study to the control of diseases and other health problems.
[†] HIPE is a computer-based system designed to collect demographic, clinical and administrative data on discharges and deaths from acute hospitals nationally. HIPE is managed by the Economic and Social Research Institute (ESRI) in association with the HSE.

Secondary Use	Example
Epidemiology	Information collected by the National Cancer Registry is used to measure the incidence and prevalence of different types of cancer. Epidemiologists can study the information collected to determine patterns in distribution and determinants of incidence of cancer cases.

The examples documented above highlight some of the valuable secondary uses of information, with appropriate steps being taken to protect the identity of the people to whom the information relates.

Information is a valuable resource, the effective use of which can lead to improvements in service delivery and quality of care. However, the conditions to be met in order to use information for these purposes vary depending on such factors as the level of risk to the privacy of the individual and the benefit to the population as a whole. For example, clinical audit is a secondary use of information directly related to the treatment of the individual - it may benefit them in the future and is typically carried out by healthcare professionals within the organisation that owe a duty of confidentiality to the patient. As such, the requirements to be met in this case are not as strict as if it was proposed to use the information for research purposes.

In order for service providers to continue to use information for the purposes outlined above, service users must be comfortable with the use of their information and need to be confident that their rights, and their identity, are being appropriately protected and respected. There is a need to strike a balance between the service user's right to personal privacy and the desirability of making information available to improve the quality and effectiveness of care through audit and research.

Failure to take all reasonable steps to protect patient confidentiality and give patients control over how their data is used risks undermining patients' confidence in the system, and their willingness to allow any access to their data. On the other hand, given the appropriate respect of their confidentiality, patients are likely to be more open to consenting to a wide range of uses of their data[11].

1.3 Secondary use of information in Ireland

The work of the Authority in this area aims to provide guidance around the precautions that should be taken, and conditions that must be satisfied, when proposing to use information for secondary purposes.

There are legislative provisions outlining the instances in which information can be used but these are somewhat ambiguous and open to interpretation. It is anticipated that the forthcoming Health Information Bill will include further provisions in respect of the secondary use of information.

The draft Heads of Bill[2] define 'secondary purposes' as relating to personal health information held for health service purposes other than primary purposes and includes research, planning, managing, delivering, auditing or evaluating existing or possible health services.

Guidance[12] has also been issued by the Office of the Data Protection Commissioner, which outlines best practice in using health information for research and audit purposes.

1.3.1 The legislation

Service users' rights, regarding the use of their information for secondary purposes, are protected in legislation. The Data Protection Acts 1988 and 2003 specify that data shall be kept for one or more specified and lawful purposes and shall not be used or disclosed in any manner incompatible with that purpose or purposes.

However, it is recognised that information is an important resource that can be used to improve service delivery and planning, and contribute to medical advancements through research. For information to be used for these purposes, service users must be in control of how the information is used and be aware of their rights in consenting or refusing to the use of their information.

Scenarios for secondary uses of information vary so vastly that decisions must essentially be made on a case-by-case basis. Best practice suggests, and the Data Protection Commissioner advises, that the most desirable approach is to obtain consent from service users when proposing to use their information for a purpose other than for which it was collected[12].

Consent, which can be either implied or explicit, can be defined as a freely given, specific and informed indication of the data subject's wishes to use their personal health information[12].

Explicit consent is consent that is clearly and unmistakably stated. It may be obtained in writing, verbally, or in any other form where the consent is clearly communicated. Where such consent is required, it should always be recorded and dated and preferably signed and witnessed[2].

Implied consent means that consent can be inferred by the actions of the service user. For example, by presenting for treatment at a General Practitioner's practice a patient is implying their consent to be treated, and by agreeing to a referral to a specialist is consenting to their information being shared for this purpose. Implied consent is typically a valid form of consent for the sharing of information within the circle of care and for purposes directly related to the provision of care such as administrative and billing purposes.

The Data Protection Commissioner advises that as much information as possible should be provided to service users in a service-user information leaflet or a statement of information practices. This should outline how data may be disclosed in the future for the benefit of the patient or for purposes not directly related to, or indeed completely separate from, the patient's own treatment.

It is anticipated that the proposed Health Information Bill will include explicit provisions governing the secondary use of personal health information. At the time of writing this review the Bill is due to be enacted in 2012.

1.3.2 Guidance available

The Data Protection Commissioner published guidance in 2007 on this topic - *Data Protection Guidelines on Research in the Health Sector*[12]. The purpose of these guidelines is to establish the basis on which research and audit can be carried out in a manner consistent with the framework of data protection legislation.

The document aims to strike an appropriate balance between the patient's right to personal privacy and the desirability of making data available for research. It strives to present a position whereby the principles of data protection can promote and work with research and clinical audit once the patient's basic right to privacy is respected.
The Data Protection Commissioner recommends anonymisation[‡] or pseudonymisation[§] (subject to adequate safeguards) as the optimal position in relation to patient identifiable information being used for secondary purposes. This is an ideal solution in cases where capturing consent is deemed particularly difficult as once information is no longer identifiable the provisions of the Data Protection Acts cease to apply.

In certain cases, anonymisation is not an option – for example, where it is essential to follow up with patients and measure the eventual outcome of their care, and for registration with disease-specific registries such as the National Cancer Registry in Ireland.

The National Cancer Registry in Ireland is in a unique position in that specific legislation allows for this function in the form of the Health (Provision of Information) Act 1997. The Data Protection Commissioner (in his Annual Report for 1997)[13] stated that the Health (Provision of Information) Act:

> "…identifies an overriding public interest – cancer prevention – and enables an exchange of personal data between data controllers which would not otherwise be permissible."

In the absence of such specific legislation, where it is necessary for the information used to be identifiable for linking or tracking purposes, the processing of the information must be undertaken with the consent of the individual involved and with the appropriate safeguards to protect their privacy and identity. It is anticipated that the proposed Health Information Bill will incorporate specific provisions in relation to data linking for which consent will not be required.

In 2010 the Authority issued guidance[3] in relation to privacy impact assessments (PIAs) in health and social care as a resource to show service providers how to ensure that they protect the privacy rights of the people using their services, and to assist them in strengthening their own governance arrangements around health information.

PIA is a process that facilitates the protection and enhancement of individuals' privacy by considering the future privacy consequences of a proposed project, for example a proposal to use information for a purpose other than for which it was originally collected.

[‡]Anonymisation results in data which is impossible to link to any known individual. This requires not only the removal of all possible identifiers, but also means ensuring that any other data or combination of data could not identify the individual.
[§] Pseudonymisation involves the use of a coding system to protect the identity of an individual to whom the information relates. Pseudonymous records are distinguishable but cannot be associated with a specific person. It eliminates the need to retain all identifying characteristics with the data.

The Authority's guidance provides a step-by-step guide on how to undertake a PIA and the important factors to be considered at each stage. A PIA, when conducted properly, will identify any actual or potential privacy concerns associated with a proposed project. The guidance is intended as a resource for all those involved in healthcare delivery, project planning and research(3).

1.4 International Review

The purpose of this international review is to identify the key themes that relate to the secondary use of information. The themes identified will inform the development of detailed IG guidance, which will assist service providers in complying with the *National Standards for Safer Better Healthcare*. They will also act as a resource for all health and social care providers seeking to improve IG practices within their organisations.

The countries that are reviewed in detail in this report are England, Canada, New Zealand and Australia. The document outlines an overview of secondary uses of personal information, legislative provisions, codes of practice and guidance available in each of the four countries.

The countries were chosen based on the results of a desktop review that identified a range of initiatives that could contribute to developing detailed IG guidance for health and social care in Ireland, particularly in respect of the secondary use of information. The developments documented in each of the countries are recent and in some cases are ongoing at the time of writing.

2. England

2.1 Introduction

The National Health Service (NHS) was established in 1948 and provides free healthcare to all residents of the UK with the exception of some dental, optical and prescription charges. The NHS is managed separately in England, Scotland, Wales and Northern Ireland but it is funded centrally through national taxation.

In England, responsibility for the NHS is devolved to ten Strategic Health Authorities (SHA) that are responsible for managing health and social care services in each of their geographical areas. The NHS is also divided into a number of Trusts, each of which is responsible for different aspects of healthcare.

Primary Care Trusts (PCTs) are responsible for providing primary and community services and for commissioning secondary care services for the residents of their respective areas. Acute Trusts, also referred to as Hospital Trusts, manage hospitals and are commissioned by PCTs to provide secondary health services.

There are a number of other types of trusts including Mental Health Trusts, Care Trusts and Ambulance Trusts[9]. There is a structured approach to IG in England at a national and local level.

2.2 Secondary use of information in England

The NHS is a source of valuable information to researchers from a range of clinical and non-clinical disciplines. NHS patient records, disease registers and databanks are vital in assessing the distribution and determinants of disease, treatment outcomes and survival rates.

The NHS established the Secondary Uses Service, which is the single, comprehensive repository for healthcare data which enables a range of reporting and analyses to support the NHS in the delivery of healthcare services. It is essentially a data warehouse that provides access to anonymous patient-based data for purposes other than direct clinical care including healthcare planning. The analyses of these types of data are important for increasing an individual's chances of surviving a disease, providing a better quality of care and improving overall public health[14].

However, in many cases, identifiable information is used for secondary purposes in which case it must be treated with the appropriate respect. A number of developments have taken place in an attempt to protect the rights of service users. Each of the following serves to protect and safeguard the rights and best interests of service users:

- Legislation
- Codes of Practice
- Guidance issued by various healthcare and regulatory bodies
- Provisions within the IG Toolkit.

Each of these will be explored in the sections that follow and a summary of the key points will then be provided.

2.3 Legislation

The legal position with regard to patient confidentiality is complex and in some areas controversial, with a number of exceptions and special cases for example, disclosures in the public interest.

However, a duty of confidentiality clearly exists and, in general, the sharing of identifiable data requires patient consent. Where the sharing of information is necessary to the provision of care to which the patient has already consented then implied consent is sufficient to share the information. Where the sharing of identifiable information is not directly related to the care of the individual explicit consent is required[15].

The Patient Information Advisory Group (PIAG) was established under the Health and Social Care Act 2001[16] to provide advice on issues of national significance involving the use of patient information and in 2008 was replaced by the National Information Governance Board (NIGB)** under the Health and Social Care Act 2008[17].

Up until December 2008, one of the functions of the PIAG was to oversee arrangements created under Section 251 of the National Health Service Act 2006[18] which allows identifiable patient information to be used for medical purposes, where it can be shown that identifiable patient data is necessary, and consent is not practicable.

For example, a research study may require access to patient identifiable data to allow linkages between different databases where the number of data subjects is too large to get consent, this would require time-limited access to identifiable information where gaining consent would not be feasible and would require more identifiable data that is necessary for the purposes of linking the data.

Each application for Section 251 support is considered carefully and a judgement made on whether the benefits of the NHS activity or proposed research are significant enough to set aside the common law duty of confidentiality in favour of the public interest[19]. On taking over this function the NIGB established a new committee, the NIGB Ethics and Confidentiality Committee (ECC) to administer applications under Section 251 on its behalf[20]. The ECC also advises on ethical issues relating to the processing of health or social care information as referred to it by the NIGB.

2.4 Codes of Practice

2.4.1 Code of Practice on Confidentiality

In 2003, the Department of Health published a code of practice for the NHS on confidentiality[7], with supplementary guidance being issued in 2010 relating to public interest disclosures[21].

The document is a guide of required practice for those who work within, or under contract to, NHS organisations concerned with personal health information. The document presents a confidentiality model which outlines the requirements that must be met in order to provide patients with a confidential service.

** The NIGB is an independent statutory body established in 2005 to promote, improve and monitor information governance in health and social care.

Record holders must inform patients of the intended use of their information, give them the choice to give or withhold their consent as well as protecting their identifiable information from unwarranted disclosures[7].

The guidance document stresses the point that patients must be effectively informed. Patients must be made aware that the information they give may be recorded, may be shared in order to provide them with care, and may be used to support local clinical audit and other work to monitor the quality of care provided.

The guidance document asks staff to consider whether patients would be surprised to learn that their information was being used in this way – if so, they are not being informed correctly. In order to inform patients properly, staff are asked to[7]:

- Check that patients have seen the available information leaflets
- Make clear to patients when information is recorded or health records are accessed
- Make clear to patients when information is or may be disclosed to others
- Check that patients are aware of the choices available in respect of how their information may be used or shared
- Check that patients have no concerns or queries about how their information is used
- Answer any queries personally or direct patients to others who can answer their questions or other sources of information
- Respect the right of patients to have access to their health records
- Communicate effectively with patients to help them understand.

The Code also emphasises consent and the fact that patients must be provided with choice. Patients have the right to choose whether or not to accept a form of care and the information disclosure needed to provide that care, and to choose whether or not identifiable information can be used for non-healthcare purposes.

While it is necessary to disclose information about a patient to those staff who are providing or auditing care, it is important to ensure that those who see information have a genuine need to do so. To this end staff must[7]:

- Ask patients before using their personal information in ways that do not directly contribute to, or support the delivery of their care
- Respect patients' decisions to restrict the disclosure and/or use of information
- Explain clearly the implications of disclosing and not disclosing.

The code of practice recommends a generic decision-support tool for sharing or disclosing information and documents examples of particular information disclosure scenarios. The issues to be considered and the appropriate steps to be taken can be determined by working through the models provided. There are important distinctions, in that the legal and ethical requirements differ in each case[7].

The models provide examples of confidentiality decisions in practice as a guide to decision-makers. It consists of three parts as follows[7]:

1. **Disclosure for healthcare purposes**: this is the disclosure of information to NHS staff involved in the provision of healthcare such as referral of a patient to a consultant. Clinical audit is also included under this heading where it is being conducted by internal clinical auditors within the NHS organisation. Every effort should be made to ensure that

patients are aware that audit takes place and that it is essential if the quality of care they receive is to be monitored and improved.

2. **Disclosure for medical purposes other than healthcare**: this is the disclosure of information to researchers for example, to a third level institute conducting research on the prevalence of diabetes in patients over fifty years of age and seeking to identify potential causal factors. It is noted that anonymised data is preferable for research purposes and where this is not possible consent must be gained. In some cases, where it is not possible to gain consent, the research may be approved if it can be justified in the public interest. Disclosure to cancer registries is also covered under this heading. The United Kingdom Association of Cancer Registries has been granted temporary statutory support to obtain patient identifiable information for use on cancer registry database, without the consent of patients.

3. **Disclosure for non-medical purposes**. This could be for example the disclosure of personal health information to the hospital chaplains. Explicit patient consent to disclose information is required for non-medical purposes.

2.4.2 The Research Governance Framework for Health and Social Care

The second edition of the Research Governance Framework for Health and Social Care[22], published in 2005 by the Department of Health, defines the broad principles of good research governance and is key to ensuring that health and social care research is conducted to high scientific and ethical standards.

The rights of the data subject are covered under ethics and responsibilities and accountability. The importance of keeping information confidential is addressed under the heading of ethics. It is noted that the appropriate use and protection of patient data is paramount. All those involved in research must be aware of their legal and ethical duties and particular attention must be given to systems for ensuring the confidentiality of personal information and to the security of those systems.

A number of responsibilities in relation to data/information are outlined as follows[22]:

- everyone involved in research with human participants, their organs, tissue or data is responsible for knowing and following the law and the principles of good practice relating to ethics, science, information, health and safety, and finance, set out in the framework
- it is essential that clear agreements describing the allocation of responsibilities and rights are reached, documented and enacted between the array of organisations and individuals that may be involved in a health or social care research study
- protecting the integrity and confidentiality of clinical and other records and data generated by research; and reporting any failures in these respects, or suspected misconduct, through the appropriate systems
- procedures are in place to ensure collection of high quality, accurate data and the integrity and confidentiality of data during processing and storage
- there are appropriate arrangements to archive the data when the research has finished, and to make it accessible
- all data and documentation associated with the study are available at the request of the inspection and auditing authorities.
- It is the responsibility of organisations providing health or social care in England to be aware of all research undertaken in their organisation, or involving participants, tissue or data obtained through the organisation.

Organisations are expected to be able to demonstrate adherence to the research governance framework. Since 2005, research governance is one of the core standards all organisations should achieve in delivering NHS care. The framework states that failure of NHS organisations to comply is to be addressed through the normal lines of accountability and performance management[22].

2.5 Guidance available

Guidelines have been issued from various sources in respect of the appropriate secondary use of information, including:

- The Information Commissioner
- The General Medical Council
- The British Medical Association

2.5.1 *Use and Disclosure of Health Data – guidance on the application of the Data Protection Act 1998*[23]

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Information Commissioner is responsible for administering the provisions of the Data Protection Act 1998[24] and the Freedom of Information Act 2000[25].

Under common law, consent must be obtained before sensitive personal data can be collected. Guidelines issued by the Information Commissioner state that information must be provided on[23]:

- the identity of the data controller
- the purposes for which the data are to be processed
- what data are to be collected
- specific disclosures that will be made
- whether any uses or disclosures are optional.

This information is referred to as "fair processing information" and can be supplied in a leaflet, a letter or as part of a medical consultation. Consent is not required when using anonymised data, when a disclosure is supported by Section 251 (as outlined in section 2.3 of this document), or for a number of limited purposes cited in the Data Protection Act, but best practice suggests that patients should still be informed.

The Information Commissioner favours anonymisation as the optimum position when using information for secondary purposes and recommends pseudonymisation where this is not appropriate.

2.5.2 The General Medical Council

The General Medical Council, the independent regulator for doctors in the UK, was established under the Medical Act 1858 and its statutory functions are today set out in the Medical Act 1983[26] as follows[27]:

- keeping up-to-date registers of qualified doctors
- fostering good medical practice
- promoting high standards of medical education and training

- dealing firmly and fairly with doctors whose fitness to practice is in doubt.

The General Medical Council issued guidance in 2009 entitled *Confidentiality*[28], which sets out the principles of confidentiality and respect for patients' privacy that doctors are expected to understand and follow. The guidance covers disclosures of information in a number of circumstances including disclosing information for research and other secondary uses.

In respect of the secondary use of information the following key points are made [28]:

- You should make sure information is readily available to patients explaining that, unless they object, personal information about them will be shared within the healthcare team, including administrative and other staff who support the provision of their care
- This information can be provided in leaflets, posters, on websites and face to face and should be tailored to patients' identified needs as far as practicable.
- In reviewing the information provided to patients, you should consider whether patients would be surprised to learn about how their information is being used and disclosed.
- You must make sure that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.
- As a general rule, you should seek a patient's express consent before disclosing identifiable information for purposes other than the provision of their care or local clinical audit.
- For many secondary uses, it will be sufficient and practicable to disclose only anonymised or coded information. When identifiable information is needed, or it is not practicable to remove identifiable information, it will often be perfectly practicable to get patients' express consent.
- You may disclose identifiable information without consent if it is required by law, if it is approved under section 251 of the NHS Act, or if it can be justified in the public interest and it is not practicable to seek consent or efforts to seek consent have been unsuccessful.
- Identifiable information should only be disclosed for research purposes where the disclosure has been approved by a Research Ethics Committee. If you are proposing to use or disclose identifiable information without consent this should be clearly stated in the proposal submitted to the Research Ethics Committee.

Supplementary guidance is available on the General Medical Council's website explaining how the principles apply in situations frequently encountered by doctors. It is stated on the website that serious or persistent failure to comply with the principles outlined in the guidance will put a doctor's registration at risk[27].

2.5.3 Guidance issued by the British Medical Association

The British Medical Association (BMA) is the independent trade union and professional association for doctors and medical students, representing doctors in all branches of medicine throughout the UK.

The Ethics Department of the British Medical Association published *Guidance on secondary uses of patient information*[29] in April 2007. In August 2011, the document was replaced by *How to respond to requests for disclosure of data for secondary purposes*[4] which outlines the conditions that must be satisfied in order for the data to be disclosed for secondary purposes, for example that any disclosure of identifiable data must meet the requirements of the Data Protection Act 1998.

In 2008 the BMA launched a confidentiality and disclosure of health information toolkit the second edition of which was published in December 2009[30]. The purpose of the toolkit is to identify the key factors that need to be taken into account when decisions are to be made about whether or not to disclose information. It consists of a series of "cards" about specific areas of confidentiality relating to children, adults who lack capacity, the deceased and the secondary uses of information[30].

The British Medical Association cautions that in the absence of patient consent, anonymised data should be used for any secondary purposes where it is practicable to do so. Some secondary uses of patient data are for social purposes unconnected with the provision of healthcare for example, for insurance or employment purposes. Such disclosures require explicit patient consent[30].

2.6 The IG Toolkit

The IG toolkit is a nationally agreed electronic self-assessment form designed to facilitate organisations to self-assess the way they handle or process information. The toolkit provides a framework to bring together the requirements, standards and best practice that apply to the handling of information[9].

All NHS organisations are required to assess their compliance with the IG requirements through the IG toolkit, and publish an annual report on compliance. The toolkit enables organisations to measure their compliance with a range of information handling requirements for example, the Data Protection Act 1988 (England) and the Information Security Management NHS Code of Practice[31].

The toolkit is constantly evolving to reflect the requirements of, and changes in, the healthcare environment, with version nine[32] being published in 2011. There are different "views" for different types of organisation, for example acute hospital trust, general practice and secondary use organisations. The toolkit consists of 45 requirements that are subdivided into six work areas as follows:

- IG management
- confidentiality and data protection assurance
- information security assurance
- clinical information assurance
- secondary use assurance
- corporate information assurance.

The following are the points that relate to the appropriate secondary use of information, with which secondary use organisations must comply[33]:

- personal information is only used in ways that do not directly contribute to the delivery of care services where there is a lawful basis to do so and objections to the disclosure of confidential personal information are appropriately respected
- where required, protocols governing the routine sharing of personal information have been agreed with other organisations
- the confidentiality of service user information is protected through the use of pseudonymisation and anonymisation techniques where appropriate.

The NHS defines a secondary use organisation as an organisation that processes patient information for secondary purposes. The term includes organisations that process national datasets, for example the NHS Information Centre for Health and Social Care. The IG Toolkit "view" is based on IG assurance within an organisation using patient information for a purpose that is not direct care.

The toolkit has continued to evolve and change annually in response to a changing IG agenda, and feedback from stakeholders. Although limited resources restrict the auditing of results, the toolkit has proved to be a useful resource in that it is a cohesive, nationally coordinated point of reference for service providers in respect of their IG responsibilities. It enables service providers to identify areas where their performance is weak and demonstrates the ways in which improvements can be made.

Audits of IG toolkit self-assessments by NHS internal auditors and external security consultants in the past have found that it is not uncommon for scores to be overstated or unsubstantiated. To ensure a common approach to information governance audits across the NHS, the Department of Health commissioned an internal audit assurance framework for the IG toolkit self-assessments in 2010[(34)]. The audit framework aims to help NHS organisations focus on what they need to do to respect patient rights, improve healthcare outcomes and maximise the benefits that can be gained from high quality and modern information technologies.

2.7 Summary

IG is a well-embedded concept in the English health and social care sector. There are detailed codes of practice covering the topic in general but also more specific guidelines governing the specific aspects of IG for example, the code of practice on confidentiality, which covers the secondary use of information. The appropriate secondary use of information and the conditions that must be satisfied in order to respect and protect the rights of service users are outlined in a number of guidance documents issued by bodies such as the Information Commissioner, the General Medical Council and the British Medical Association.

This gives credence to the fact that the secondary use of information is widespread, holds enormous potential, and attempts to cater for the different scenarios that medical professionals may face in the course of their work.

The following is a summary of key developments that have taken place around the secondary use of information in terms of guidance available and key principles that have emerged in England:

- The Department of Health's code of practice on confidentiality emphasises the point that patients must be effectively informed of the ways in which their information will be used and must be given the opportunity to object to any of these uses. The code also presents a model for guiding health professionals in their decisions on whether or not to disclose personal information outlining different scenarios differentiating between use for healthcare purposes, use for medical purposes other than healthcare and use for non-medical purposes

- Guidance for doctors issued by the General Medical Council and the British Medical Association, which again emphasise the importance of informing patients, for example through leaflets in the waiting room. The guidance documents also identify situations in which explicit patient consent is required and how to proceed if this is not possible

- The IG toolkit now includes secondary use organisations as one of the organisation types and includes a set of 30 IG requirements which they must meet. This reinforces the point that the secondary use of information requires a specific set of safeguards in order to ensure the appropriate respect is afforded to those whose information is being used.

3. Canada

3.1 Introduction

Canada's population of approximately 34 million people is governed as a parliamentary democracy consisting of a federation of ten provinces and three territories. The federal government is responsible for matters that concern Canada as a whole, such as international trade and national defence.

Provincial and territorial governments fund and are responsible for the administration and provision of healthcare and social services in their respective areas. However, the provinces and territories do not have exclusive legislative powers, as they also receive funding that is dependent on compliance with the Canada Health Act 1984[35].

There is considerable variety in the types, sizes and complexity of IG structures within which healthcare providers and healthcare organisations operate in Canada. There are a number of pan-Canadian IG mechanisms in place; however most of the provincial structures and systems are by no means nationally cohesive. This is primarily due to legislative differences between the provinces. However, efforts are being made to move towards a more inclusive, pan-Canadian approach to IG.

3.2 Secondary use of information in Canada

The challenge facing Canada, and other jurisdictions, is to reach a workable and practical balance between the value people place on improvements in health and social care that can be gained from research on the one hand, and the value they place on the privacy and confidentiality of their information on the other[36]. These rights are constitutionally enshrined in the *Canadian Charter of Rights and Freedoms* and Quebec's *Charter of Human Rights and Freedoms*[37].

In 2007, Canada Health Infoway published a white paper on information governance of the interoperable electronic health record (EHR)[38]. The white paper identifies the secondary use of information as one of the core IG topics relating to the privacy rights of patients. Although the EHR raises fresh challenges in this regard, the issues and concerns also exist and must be addressed in the context of paper health records.

At the time of writing this report concerns and safeguards surrounding the secondary use of health information are to the fore in Canada as is reflected in recent changes to policies. The Canadian Institute for Health Information (CIHI), which will be explored in detail in section 3.4, updated its privacy policy in 2010 to clearly distinguish between the collection, use and disclosure of identifiable information and de-identified information.

The College of Physicians and Surgeons of Alberta launched a data stewardship framework for the secondary use of health information in December of 2009. Alberta will be explored as an example of provisions in pace at a state level.

Each of the following serves to protect and safeguard the rights and best interests of service users:

- Legislation
- Provisions in place by the Canadian Institute for Health Information
- The Pan-Canadian Health Information Privacy and Confidentiality Framework
- The Alberta data stewardship framework

Each of these will be discussed in the sections that follow and a summary of the key points will then be provided.

3.3 Legislation

Data protection legislation has emerged across Canada with different requirements applying at provincial, territorial or federal level. However, health services and population health research frequently cross provincial and even national borders. As such, some studies can potentially invoke multiple laws with varying and sometimes inconsistent legislative provisions[36].

Despite the fragmentation of legislation most data protection laws are generally modelled on the internationally accepted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[39] developed by the Organisation for Economic Cooperation and Development (OECD) in 1980. The Canadian Standards Association has reformulated these guidelines into the *Model Code for the Protection of Personal Information*[40]. This Code has been formally incorporated as Schedule 1 of the Personal Information Protection and Electronic Documents Act (PIPEDA)[41]. PIPEDA applies to both federal and provincial entities.

Canada has two federal privacy laws - the Privacy Act[42] and the Personal Information Protection and Electronic Documents Act (PIPEDA)[41]. The Privacy Commissioner of Canada is responsible for the enforcement of both.

The Privacy Act came into effect in 1983 and imposes obligations on specific federal government departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information, including health information. It gives individuals the right to access, and request correction of, personal information about themselves held by these organisations[43]. PIPEDA confers these obligations on private sector organisations also.

Canadian privacy laws impose a legal obligation on health information custodians and trustees to identify the purpose, for which they collect, use and disclose, or retain information. This may include purposes other than treatment and care; so-called secondary purposes, for example research. Information notices given to patients, are intended to give individuals a sense of what uses are permissible[38].

3.4 The Canadian Institute for Health Information

The Canadian Institute for Health Information (CIHI) is an independent, not-for-profit organisation that provides data and analysis of the Canadian health system and the health of Canadians[44]. CIHI has offices in Ottawa, Toronto, Montreal, Edmonton and Victoria and analyses health information and data received from hospitals, regional health authorities, medical practitioners and governments.

Although not involved in the provision of direct clinical care, CIHI analyses a large volume of patient identifiable health information, which presents a challenge in terms of ensuring this information is properly protected.

CIHI seeks to protect the privacy of information when it is used for secondary purposes through the following channels:

- comprehensive privacy policies that are regularly reviewed and updated
- complying with legislative provisions in allowing it's privacy and security practices to be audited
- data sharing agreements
- undertaking audits on third party data recipients to ensure they meet their contractual obligations.

3.4.1 Comprehensive privacy policies

CIHI maintains a comprehensive privacy programme as the protection of individual privacy, the confidentiality of records and the security of information are essential to their operations.

A cornerstone of this programme is a set of strict principles and policies that govern how CIHI collects, stores, analyses and disseminates data. These are outlined in the documents, *Privacy and Security Framework*[45] and *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010*[46].

The 2010 privacy policy was a result of a review of CIHI's privacy and security arrangements by the Ontario Information and Privacy Commissioner as part of the renewal of its prescribed entity process under Ontario legislation. One of the recommendations was that CIHI update its privacy policy specifically to clearly distinguish between the collection, use and disclosure of identifiable information and the collection, use and disclosure of de-identified information.

The updated policy was approved in March 2010 and implemented across the organisation[47]. Although these policies have been developed specifically by CIHI they are aligned with the federal Personal Information Protection and Electronic Documents Act (PIPEDA)[48]. As such they could be used as a basis for other organisations developing a suite of IG policies and procedures, particularly in relation to provisions around the secondary use of information.

3.4.2 Legislative obligations

CIHI is recognised as a prescribed entity in legislation in a number of provinces, for example in Ontario's *Personal Health Information Protection Act*[49]. CIHI's prescribed entity status enables it to collect information in those provinces without patient consent. Each of the statutes also prescribes strict safeguards with respect to disclosing information to CIHI. These safeguards include, for example, the necessity of having agreements in place between CIHI and the disclosing province and the right of the province to impose requirements on CIHI's information management practices, such as having the right to audit CIHI's privacy and security practices[47].

3.4.3 Data sharing agreements

Legislation in the jurisdictions is increasingly dictating the need for CIHI to enter into data-sharing agreements. CIHI enters into data-sharing agreements and other legal arrangements with governments and other entities to provide for the collection, use and disclosure of information in accordance with CIHI's privacy and security framework. A list of third parties with which agreements have recently been reached are included in CIHI's Annual Privacy Report 2009-2010[47].

3.4.4 Audits of third party data recipients

In an attempt to further safeguard the information in use, and improve overall IG, CIHI also undertakes audits on third party data recipients. The privacy audit programme is designed to ensure that external third parties who enter into an agreement with CIHI meet their contractual obligations.

The audits allow CIHI to collaboratively verify the manner in which external recipients handle personal data provided by CIHI. In addition, the audits provide the added educational value of identifying best practices and strengthening those policies, procedures and practices that could more adequately protect the information of Canadians[47].

3.5 The Pan-Canadian Health Information Privacy and Confidentiality Framework

In an attempt to harmonise existing Canadian privacy regimes, the Federal/Provincial/Territorial Conference of Deputy Ministers of Health tasked its Advisory Committee on Information and Emerging Technologies (ACIET)[††] with developing a *Pan-Canadian Health Information Privacy and Confidentiality Framework* ("the ACIET Framework")[50]. The *ACIET Framework* provides guidelines for common and consistent statutory provisions for the collection, use and disclosure of information.

The framework applies to both the public and private healthcare sectors and although it is a guide rather than a prescription, it serves as a tool for regulators as they seek to develop consistent privacy requirements through the introduction or amendment of health privacy legislation.

The *ACIET Framework* was finalised in January 2005 and endorsed by the Federal/Provincial/Territorial Conference of Deputy Ministers of Health, with the exception of Saskatchewan and Quebec. The *ACIET Framework* continues to serve to inform and influence the development and review of health privacy statutes in Canada[38].

[††] In December 2002, the Federal/Provincial/Territorial Deputy Ministers of Health created the Advisory Committee on Information and Emerging Technologies (ACIET). The Advisory Committee's mandate is to provide policy development and strategic advice on health information issues and on the effectiveness, appropriateness and utilization of emerging health products and technologies to the Conference of Federal, Provincial, and Territorial (F/P/T) Deputy Ministers of Health.

It is noted within the framework that[50]:

> "Express consent must be obtained for the collection, use or disclosure of personal health information for purposes outside the circle of care, except as specifically otherwise provided by legislation."

3.6 Alberta approach to the secondary use of health information

As previously mentioned, the legislation and subsequent policies and procedures are fragmented in Canada with little cohesion at the federal level. As such a number of provinces have proceeded to develop their own structures and processes to deal with IG issues. One such province is Alberta.

In 2006, the College of Physicians and Surgeons of Alberta published its *Data Stewardship Framework*[51] in an attempt to provide clear guidelines for the profession on the management of health information. In 2009 the college produced supplementary guidance – a framework for the secondary use of health information[5].

It is noted in the framework that a balance must be achieved between the positive rights of society and the rights of a patient to privacy and confidentiality. Fundamental to this balancing is the ethical use of information and the professional conduct of all the parties involved, and an effective oversight of the entire process to ensure there are appropriate controls.

The college identifies the following as secondary use principles[5]:

- respect for personal privacy
- openness and transparency of all secondary uses
- oversight and accountability
- patient, health system or social benefit
- balance and reciprocity
- use non-identifiable information.

Secondary uses require boundaries and guidelines to offset the inherent loss of personal privacy. In order to respect personal privacy there must be[51]:

- an explicitly defined secondary use and purpose
- a clear public interest and material value for the defined secondary use
- the least restrictive or coercive methods necessary to achieve the defined purpose
- an ethical framework to balance the public good with the individual loss of privacy
- adequate security and safeguards
- the most limited scope of data necessary to achieve the defined purpose
- the most limited personal identification necessary to achieve the defined purpose
- legal remedies for breaches.

The document sets out secondary use guidelines for physicians. Physicians who contemplate using data for secondary purposes are expected to perform a level of due diligence. This is both a legal and a professional obligation.

The level of due diligence and competence must be commensurate with potential risks, fulfil legal and ethical duties, and should at a minimum include[51]:

- definition of the purpose and data requirements of the secondary use
- assessment of the ethical considerations
- establishment of the consent model, and engagement of an approval and oversight process as required
- establishment of the data and security controls.

The document notes that unless required or permitted by law, all approved secondary uses should generally be for the direct benefit of patients, or an indirect benefit to the public through quality improvement of the system. There must be an appropriate balance of the potential benefit, the burden to enable the secondary use, and the expectation that the objectives can be reasonably achieved.

3.7 Summary

The challenge of achieving a balance between the value people place on improvements in health and social care that can be gained from secondary use of information and the value they place on the privacy and confidentiality of their information has been recognised in Canada.

The following is a summary of the key developments that have taken place around the secondary use of information in terms of the guidance available and the key principles that have emerged:

- Canada privacy laws impose a legal obligation on health information custodians and trustees to identify the purpose for which they collect, use, disclose and retain information. Information notices should be given to patients to give them a sense of what uses of their information may occur.

- CIHI is an example of an organisation that uses information for secondary purposes and has comprehensive privacy policies and data sharing agreements in place to ensure that information is collected, used and disclosed in a manner consistent with legislation, guidelines and recognised best practice. CIHI also conducts audits of third party data recipients.

- The Pan-Canadian Health Information Privacy and Confidentiality Framework addresses the issue of consent where it is proposed to use information for purposes outside the circle of care.

- Policies and procedures have been developed at the state level for example the secondary use principles and guidelines documented in the Data Stewardship Framework in Alberta.

4. New Zealand

4.1 Introduction

New Zealand has a population of approximately 4 million and is governed by a parliamentary democracy system. The government is fully integrated nationally with no separate states or territories[52]. The Minister of Health in New Zealand has overall responsibility for the health and disability system.

The health service is funded and delivered by 21 district health boards (DHBs) who report directly to the Minister of Health[53]. Recent changes to the Ministry of Health structure include the creation of a National Health Board (NHB) to improve coordination between the 21 DHBs.

The New Zealand health system is one that has undergone a number of reforms and transformations in the past number of years – particularly in relation to health information governance structures. The Working to Add Value through E-information (*WAVE) Report - From Strategy to Reality*[54], published in 2001, made 79 recommendations towards improving the quality of New Zealand health information management and ultimately the quality of healthcare throughout the country.

In 2005, a *Health Information Strategy for New Zealand* was launched resulting in the restructuring of a number of health information committees[55], with transformations ongoing at the time of writing this report.

At the time of writing this report, the New Zealand health agenda is very much focused towards e-health. However, similar IG issues exist whether in respect of paper or electronic records. The secondary use of information and concerns around privacy in this regard are coming increasingly to the fore as the country moves closer to the widespread use of electronic health records.

4.2 Secondary use of information in New Zealand

The Code of Health and Disability Service Consumers' Rights[56] is a regulation issued in 1996 under the Health and Disability Commissioner Act 1994[57]. It sets out ten rights applicable to all health and disability consumers, including those involved in research.

Two of these rights are particularly relevant to the secondary use of information: the right to be treated with respect and the right to be fully informed. The right to be treated with respect specifically states that consumers have the right to have their privacy respected.

The right to be fully informed includes notification of any proposed participation in teaching or research, including whether the research requires, and has received, ethical approval. Before making a choice or giving consent, every consumer has the right to the information they need to make an informed choice or give informed consent[56]. This Code underpins the various guidance documents that have been developed subsequently.

A further document of interest is that produced by the Palliative Care Council of New Zealand[‡‡] in 2010 outlining concerns about the security and privacy of individuals' health information.

Although it is not a guidance document, it provides a useful insight into the attitude of New Zealanders towards the use and sharing of their information and addresses a number of concerns raised. The document summarises the results of previous research undertaken on attitudes to sharing of health information in New Zealand.

The authors report on surveys conducted in 2006 and 2009 by Whiddett et al.[58] and Hunter et al.[59] respectively. The surveys explored varying levels of agreement and comfort about health information sharing among the general public. Findings from the studies indicated that the role of the person requesting the information, content of the information, and level of identification of health information were all important modifiers of willingness to allow sharing of information.

The authors surmise that a key message for health professionals and health and disability service providers is that people feel that their health information belongs to them, and healthcare providers must act as responsible custodians of that information. In addition, the New Zealand public does want to be informed about how their information is going to be used, as well as being given the opportunity to consent, or not, to those uses[60].

There are a number of sources of reference for service providers, and service users, in respect of the topic, which build on each other and convey similar themes and issues to be addressed. These include:

- Legislation
- *The Health Information Privacy Code*[61]
- Guidance issued by the Office of the Privacy Commissioner[62-65]
- Guidance issued by the National Ethics Advisory Committee[8].

Each of these is explored in the sections that follow and a summary of the key points is then provided.

4.3 Legislation

Legislatively, it is the Privacy Act 1993[66] which is of primary importance in New Zealand. The Privacy Act 1993[66] sets out twelve information privacy principles on collecting, using, keeping, disclosing, transferring, accessing and securing personal information[67]. In respect of the secondary use of information it is principles ten and eleven that are of primary importance. Principle ten places restrictions on the use of personal information while principle eleven places limits on the disclosure of personal information.

The provisions of the Privacy Act are administered by the Privacy Commissioner. The Privacy Act make provision that any code of practice based on the Act developed by the Privacy Commissioner for a specific sector, would become lawful[68]. One such code is the *Health Information Privacy Code 1994*[61], which was revised in 2008.

[‡‡]The Palliative Care Council (PCC) was established in 2008 by Cancer Control New Zealand to provide independent and expert advice to the Minister of Health, and to report on New Zealand's performance in providing palliative and end of life care.

This means that the rules contained within the *Health Information Privacy Code*[61] are legally binding. The code sets specific rules for health sector agencies to ensure the protection of individuals' personal information. In the health sector, the code takes the place of the Privacy Act's information privacy principles, and deals with information collected, used, held and disclosed by health agencies.

4.4 *The Health Information Privacy Code 1994*

The *Health Information Privacy Code 1994*[61], published by the Office of the Privacy Commissioner, which was updated in 2008, applies specific rules to agencies in the health sector to better ensure the protection of individual privacy. With respect to health information collected, used, held and disclosed by health agencies, the code supersedes the twelve information privacy principles in the Privacy Act[68].

It modifies the information privacy principles in the Privacy Act[66] by applying the rules specifically to health information and health agencies. The code regulates how health agencies collect, hold, use and disclose health information about identifiable individuals.

The code also includes a commentary around each rule which acts as guidance for organisations, explaining how to comply with the rules. The code has formed the basis for a number of sources of guidance developed for health and social care providers and professionals, for example those produced by the Office of the Privacy Commissioner.

4.5 The Office of the Privacy Commissioner

The Privacy Act 1993 is administered by the Privacy Commissioner. The Privacy Commissioner's Office has a wide range of functions including investigating complaints about breaches of privacy and examining proposed legislation and the impact it may have on individual privacy[69].

In respect of the privacy of health information the Privacy Commissioner has produced a number of documents and resources that offer guidance to health and social care professionals, with provisions around the secondary use of health information being addressed.

In May 2011, the Privacy Commissioner launched a health privacy toolkit aimed at health consumers and health providers. It brings together new guidance material with the material the office has previously produced and puts it all together in one place as a single point of reference for service providers. Included in the health privacy toolkit are:

- the *Health Information Privacy Code*[61]
- a series of health information privacy fact sheets[63-65]
- *On the Record: A Practical Guide to Health Information Privacy*[62]
- health-related privacy case notes[70] (summaries of health-related privacy complaints).

4.5.1 Health Information Privacy Fact Sheets

The Office of the Privacy Commissioner has produced a series of five fact sheets, available on the Commissioner's website (www.privacy.org.nz), relating to the health information privacy code, that cover the following areas:

- a general overview of health information privacy
- collection of health information
- disclosure of health information
- dealing with requests for health information
- storage, security, retention and disposal of health information.

The Privacy Commissioner notes that there are two key concepts addressed in the health information privacy code[61] – purpose and openness[63]. The first means that agencies must know why they are collecting health information and only collect the information they need. Once health information has been collected for a particular purpose, it can be used or disclosed for that purpose without additional consent.

The concept of openness requires agencies to let patients know how their information is going to be used and disclosed so that patients can make informed decisions about whether or not to provide it[63]. Both of these concepts are central to the appropriate use of health information for secondary purposes. There are twelve rules within the code, two of which relate strongly to secondary use of information:

- tell people how you are going to use their information
- use information for the purpose you collected it.

Where a health agency collects health information directly from the individual concerned, the health agency must take steps to ensure that the individual is aware of why the information is being collected, how it will be used and by whom and their rights as provided for in the health information privacy code. The Privacy Commissioner notes that this explanation to service users could be a paragraph or two, on a form, a poster on the wall, or a conversation with the patient. It should happen before the health information is collected or as soon as possible afterwards. However, repeat explanations are not necessary[64].

The disclosure of health information is always allowed when the person concerned or their representative has given their permission or where the disclosure was one of the purposes for which the information was originally obtained. For example, if a doctor collects information from a patient to pass on to a specialist there is no need to get the patient's permission for that disclosure because disclosure was one of the reasons for collection. However, the patient would normally have to be told the disclosure was going to occur[65].

4.5.2 *On the Record: A Practical Guide to Health Information Privacy*[62]

The third edition of *On the Record: A Practical Guide to Health Information Privacy*[62] was published by the Office of the Privacy Commissioner in 2011. It follows on from previous versions published in 1999 and 2000 recognising that the health environment has changed substantially since these earlier editions.

On the Record[62] is a ready-reference guide for managing common situations that people in the health sector face. It uses examples to illustrate how privacy law works and gives advice on developing policies.

A key concept reinforced in *On the Record*[62] is the need to be open with the people from whom the information is being collected. It is noted that if this is done people will not be taken by surprise later which can lead to distress and complaints. This document highlights that it is best to have clear policies around use and disclosure so that the agency and patients alike are clear about who has access to information and why.

In general, *On the Record* emphasises thinking ahead, taking reasonable steps to anticipate how information is going to need to be used and disclosed, and then telling patients about those potential uses and disclosures[62].

4.6 The National Ethics Advisory Committee

The National Ethics Advisory Committee's (NEAC) statutory functions are to provide advice to the Minister of Health on ethical issues of national significance regarding health and disability research and services, and to determine nationally consistent ethical standards and provide scrutiny for such research and services[§§].

In December 2006, the NEAC produced ethical guidelines for observational studies[***(8)]. The document is primarily intended to guide investigators conducting observational studies, including audits and related activities. The guidelines base their requirements for ethical review on the principle that intensity of ethical scrutiny should be proportionate to the level of risk of the activity.

On this basis they state that: "observational research requires ethics committee review; audits and related activities do not require ethics committee review unless there is a specified requirement for this; and public health investigations do not require ethics committee review"[8].

The document states that audits and related activities, for example clinical audits within a hospital setting, do not require ethics committee review unless they reach a particular threshold of risks. The activity should be conducted by people who are under a professional or an employment obligation to maintain patient confidentiality.

The justification for this is that the use is related to the primary purpose of data collection, and in such settings only individuals bound by a professional or an employment obligation to preserve confidentiality should have access to identifiable or potentially identifiable information[8].The document echoes the point of open communication with service users that is a recurring theme throughout the guidance explored in the course of this research.

[§§] The NEAC was established under section 16 of the New Zealand Public Health and Disability Act 2000 and its first members appointed in 2001. NEAC has up to 12 members who are appointed by the Minister of Health for a term of up to three years[71]

[***] In observational studies the investigators observe and analyse information about health or disability but do not alter the care or services that people receive. They include epidemiological and clinical observational research as well as audits and related activities[8].

The document also notes that service providers should inform the public that observational studies are essential for the high-quality delivery of health or disability services, and that their information may be used for such purposes.

4.7 Summary

The following is a summary of the key developments that have taken place around the secondary use of information in New Zealand in terms of the guidance available and the key principles that have emerged:

- The right to privacy and the right to be fully informed form part of the Code of Health and Disability Service Consumers' Rights in New Zealand.
- The Health Privacy Code applied 12 specific rules to agencies in the health sector to better ensure the protection of individual privacy. Two of the rules are particularly relevant to the appropriate secondary use of information – tell people how you are going to use their information and use information for the purpose you collected it.
- In May 2011 the Privacy Commissioner issued the health privacy toolkit, which brings together new guidance material with the guidance already published by the office and puts it all together in one place as a single point of reference for service providers.
- The Health Privacy Code and other guidance documents emphasise the importance of being open with service users about how their information is going to be used.

5. Australia

5.1 Introduction

Australia operates a federal system of government in which power is divided between the Commonwealth Government and the six state governments. The Commonwealth Government is responsible for passing legislation relating to issues that concern Australia as a whole such as taxation, defence and foreign affairs.

The states retain legislative power over all other matters that occur within their borders, including education and health. Each state has its own constitution. Three of the ten territories have been granted a limited right to self-government by the Commonwealth and a range of issues are now handled by a locally-elected parliament.

The other seven territories continue to be governed by Commonwealth law. While overall coordination of the public healthcare delivery system is the responsibility of federal, state and territory health ministers, the health service in Australia is governed centrally by the Department of Health and Ageing. The Department has responsibility for providing leadership in policy making, research and national health information management[3].

The significance of health information, the role it plays in ensuring high level quality and safety, and appropriate governance structures has been on the Australian health agenda since the 1993 National Health Information Agreement (NHIA)[72]. The latest version of this agreement came into effect in September 2004.

5.2 Secondary use of information in Australia

The basis for governing the secondary use of health information in Australia is primarily legislation in the form of the federal privacy act and state-level legislation in respect of privacy and specific health information legislation that has been developed in most states at the time of writing this report.

Privacy principles form part of the legislative provisions at the federal level and separate codes of practice and guidelines have also been developed at a state level based on state specific legislation. This has led to a patchwork of principles and guidelines on privacy of information in general. The governance structure and the types of health and social care organisations the legislation applies to has been the cause of further confusion as principles and sources of guidance are further divided in terms of the public and private sector.

In recognition of the problems this has caused there have been moves in recent times towards developing a more structured and cohesive national approach to privacy and the use of health information.

The secondary use of health information will be discussed in the context of:

- Legislation
- Privacy principles
- The Australian Commission on Safety and Quality in Health Care
- Use of health information in private medical practice
- Examples of guidance at state level.

A summary of the key points will then be provided.

5.3 Legislation

In a speech given to the Medico Legal Congress in 2008 the Acting Deputy Director of the Policy Office of the Privacy Commissioner[†††] noted that the fundamental difficulty with Australian privacy legislation is not the content or the principles within it but the existence of multiple and overlapping regulatory standards[(73)].

The Acting Deputy Director noted that health privacy regulation and privacy laws generally need to be clearer and simpler than the current scenario of regulatory overlap and multiple sets of privacy principles at the Commonwealth, state and territory levels[(73)].

Legislation will be discussed under the following headings:

- Federal legislation
- State legislation
- Legislative reform.

5.3.1 Federal legislation

The relevant federal legislation is the Privacy Act 1988[(74)] and the Privacy Amendment (Private Sector) Act 2000[(75)]. The Privacy Act has regulated the handling of personal information held by all health service providers in the private sector since 2001. This includes GPs, private hospitals, pharmacists and allied health professionals. It does not cover public healthcare providers such as public hospitals or their staff, which are instead governed by state or territory legislation. A number of states have also enacted specific legislation to govern their private sector health providers[(73)].

There are currently two separate sets of principles – Information Privacy Principles and National Privacy Principles set out in the Privacy Acts. The Information Privacy Principles applies to Commonwealth and public sector agencies and the National Privacy Principles (set out in the Privacy Act) applies to private sector organisations. This is a result of how the Act has evolved since its inception in 1988.

However, there appears to be no rationale for maintaining this dual approach and calls have been made to develop a unified set of privacy principles for a more consistent national approach to privacy regulation. It is anticipated that this will have a trickle down affect to legislation and regulation at the state level also.

5.3.2 State legislation

As in Canada, there is no specific health information legislation at a national level. In the absence of this some states and territories have enacted specific health information legislation[(67)]. One example is the New South Wales Health Records and Information Privacy Act 2002[(76)].

[†††] In November 2010 the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner.

The Health Records and Information Privacy Act 2002[76] (HRIP Act) came into effect in September 2004. It governs the handling of health information in the public sector and it also seeks to regulate the handling of health information in the private sector in New South Wales (NSW).

In December 2004, the Office of the Privacy Commissioner in New South Wales developed four statutory guidelines under the HRIP Act. These guidelines are legally binding documents that define the scope of particular exemptions in the health privacy principles in the following areas[77]:

- Use or disclosure of health information for the management of health services
- Use or disclosure of health information for training purposes
- Use or disclosure of health information for research purposes
- Notification when collecting health information about a person from someone else.

5.3.3 Legislative reform

The Australian Law Reform Commission (ALRC)[‡‡‡] promotes national consistency in relation to the privacy of health information. In 2008 the ALRC published *For Your Information: Australian Privacy Law and Practices*[79].

The document presents the findings of an inquiry into the extent to which the Privacy Act and related laws continue to provide an effective framework for the protection of privacy in Australia. The final report contained 295 recommendations to the Government. With respect to the privacy and secondary use of health information the following are the key recommendations[79]:

- Develop a single set of privacy principles to replace the IPPs and the NPPs
- Enhance and clarify the protections around the sharing of health information and the ability to use personal information to facilitate research in the public interest.

The Government has acknowledged that where it accepts the recommendations relating to health services and research the recommendations will be implemented in the amendment to the Privacy Act.

The Government agreed with the recommendation to develop a single set of Australian Privacy Principles to replace the existing sets. A draft version of these was published in June 2010[80] and it is anticipated that they will form a key part in amendments to the Privacy Act. It was stated within the document outlining the draft Australian Privacy Principles that another document is to be released for public consideration outlining specific privacy protections for information relating to health. At the time of writing this report no such document has been released.

[‡‡‡] The Australian Law Reform Commission (ALRC) is a federal agency that reviews Australia's laws to ensure that they provide improved access to justice for all Australians by making laws and related processes more equitable, modern, fair and efficient[78]. The ALRC makes recommendations to government so that the government can make informed decisions about law reform. Although the ALRC's recommendations do not automatically become law the Commission has a strong record of its advice being accepted with over 85% of its reports being either substantially or partially implemented[78].

5.4 Privacy Principles

At present, there are two sets of privacy principles in Australia – the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) – both of which are contained in legislation in the form of the Privacy Act and the Privacy Amendment (Private Sector) Act respectively.

The IPPs are the baseline privacy standards applicable to Australian public sector agencies (but do not apply to public health providers as these are governed by state law) and the NPPs confer similar obligations on private sector organisations – including health service providers. There have been recent calls to simplify privacy regulation with recommendations being made by the ALRC to develop one set of privacy principles to replace the IPPs and NPPs in a move toward a more consistent approach.

5.4.1 Information Privacy Principles

Information Privacy Principles (IPPs) are the baseline privacy standards applicable to public sector agencies. A number of the principles are specifically applicable to the secondary use of information. Principle two relates to the solicitation of personal information from the individual concerned and requires that the collector ensures that the individual is generally aware of[81]:

- The purpose for which the information is being collected
- If the collection of the information is authorised or required by or under law – the fact that the collection of the information is so authorised or required
- Any person to whom, or any body or agency to which, it is the collector's usual practice to disclose personal information and any person, body or agency to whom that first mentioned body typically passes on that information.

Principle nine states that personal information is only to be used for relevant purposes. A record-keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant[81].

Principles ten and eleven place limits on the use of personal information stating that a record-keeper who has possession or control of a record containing personal information that was obtained for a particular purpose shall not use the information for any other purpose unless[81]:

- The individual concerned has consented to the use for the other purpose
- The purpose for which the information is used is directly related to the purpose for which the information was obtained
- There is a justification for release of the information in the public interest, or where the use is required or authorised by law.

5.4.2 National Privacy Principles

The National Privacy Principles (NPPs) are applicable to private sector organisations. Principle two of the NPPs confers similar obligations on private sector organisations in respect of the secondary use of information.

5.4.3 Proposed Privacy Principles

The June 2010 release of Draft Australian Privacy Principles[80] marked the first step in the Australian Government's implementation of the announced reforms to the Privacy Act. It is anticipated that the Australian Privacy Principles, as the cornerstone of the privacy protection framework, will appear as one of the first parts in the new Act. The structure in which the Australian Privacy Principles appear is intended to reflect the cycle that occurs as entities collect, hold, use and disclose personal information.

Principle 5 relates to the notification of the collection of personal information. It places an obligation on entities to ensure that an individual is aware of certain matters at the time of collection of the personal information of the individual. The notification principle requires that the individual will be made aware of how and why personal information is, or will be, collected and how the collecting entity will deal with the personal information[80].

Principle 6 covers the use or disclosure of personal information. It sets out the circumstances in which entities may use or disclose personal information that has been collected or received. It is implicit from the principle that entities may use or disclose personal information for the primary purpose for which the information was collected. Generally, personal information should only be used or disclosed for purposes other than the primary purpose, that is, for a secondary purpose, if the relevant individual has consented[80]. There are however a number of exceptions to this, for example disclosure in the public interest.

The Acting Deputy Director of the Policy Office of the Privacy Commissioner noted that if a single set of privacy principles were to be enacted under the Privacy Act it is likely that the states and territories would mirror these principles to regulate their own public sectors – including health. As state privacy laws govern public hospitals this would bring Australia significantly closer to achieving the aim of national consistency both across the public and private sectors and also across Commonwealth, state and territory jurisdictions[73].

5.5 Use of information in private medical practice

In line with the provisions of the Privacy Act 2000[75], private medical practitioners must comply with the National Privacy Principles. In 2002 the Royal Australian College of General Practitioners produced a *Handbook for the Management of Health Information in Private Medical Practice*[§§§(6)].

The handbook was developed as a best practice model to assist medical practitioners in complying with their legal and ethical obligations in relation to the privacy and confidentiality of information. The importance of openness with patients in terms of how their information is used is reiterated throughout the document and can be clearly identified as the key point to be taken from the handbook.

The authors identify consent as the guiding principle for medical practitioners when obtaining information from their patients, using that information, or disclosing the information to other people.

[§§§] A review of the handbook commenced in 2009 but was put on hold due to the review of privacy legislation of the ALRC and pending the associated amendments to the Privacy Act. In the interim the College recommends the continued use of the 2002 version until the updated version reflecting changes in legislation is ready to be released.

The handbook states that as a general rule it is likely that the consent requirements will be satisfied as long as the medical practitioner is open with patients about how their information is to be used. It is important to ensure there are shared expectations between the medical practitioner and the patient about how information will be used.

Medical practices must have a written policy for their management of information which is readily available to all patients. This will assist patients in understanding how their information may be used if the key elements of the policy are outlined in a patient information leaflet or newsletter.

The policy is based on the concept of keeping the patient informed through readily accessible information leaflets and through discussions during consultations. This reduces the likelihood of grievances at a later stage if information is used in a way that a patient might not have expected.

In addition, the culture of openness and transparency means patients are more likely and willing to share their information which leads to improved quality of care for them and also facilitates the appropriate secondary use of health information in a way that patients are comfortable with.

The document explores what steps medical practitioners should take and what safeguards need to be put in place when proposing to use information for:

- Teaching purposes
- Research
- Quality assurance and continuing professional development.

5.5.1 Teaching purposes

The use of information for teaching purposes raises particular privacy concerns as patients are often not aware that their information may be used in this manner. Wherever possible, information should be de-identified before it is used for teaching purposes. Where this is not possible the doctor must be certain that the patient understands and agrees to this use[6].

5.5.2 Medical research

Information can be used within a practice for the purposes of medical research with the express consent of the patient, or where the research is directly related to the purpose for which the information was collected from the patient. In all other cases the research must be approved by a Human Research Ethics Committee and must comply with that committee's requirements[6].

Where there is a doubt as to whether the proposed research is directly related to the purpose for which the information was collected express patient consent should be obtained in writing. All research records should be de-identified at the earliest time possible consistent with the proper conduct of the research. Where de-identified information is used best practice suggests that patients of the practice should still be informed. Patients can be made aware of this through an information sheet in the waiting room[6].

5.5.3 Quality assurance and continuing professional development

The importance of quality assurance and continuing professional development activities in promoting and maintaining high quality healthcare are well documented. However, many patients may not understand what these activities are or that they may involve people other than their treating medical practitioner accessing their medical records. It is therefore important to make patients aware that these activities are carried out as part of the normal functioning of the practice[6].

This can be achieved through the distribution of patient information leaflets explaining the activities undertaken by the practice, and through direct discussion with patients. As a result this will mean that the patient will expect such ongoing activities around their health information and appreciate the associated benefits of improved quality in healthcare delivery.

Information can be used for quality assurance and continuing professional development activities within the practice where[6]:

- The activities are directly related to the purpose for which the information was collected and are within the reasonable expectations of the patient
- The patient has given express consent for the use of their information for these activities
- The information has been de-identified
- The activities involve research or the compilation of statistics, have been approved by the Human Research Ethics Committee and are conducted in accordance with that committee's requirements.

5.6 The Australian Commission on Safety and Quality in Health Care

The Australian Commission on Safety and Quality in Health Care was established in January 2006 and officially commenced as an independent statutory authority in July 2011, under the National Health and Hospitals Network Act 2011. The role of the Commission is to lead and coordinate improvements in safety and quality in healthcare across Australia. The establishment of such a body represents a further attempt towards coordination and cohesion of health services and associated policies and procedures across all states and territories.

In 2008, Australian Health Ministers endorsed the Commission's *Australian Charter of Healthcare Rights*[82] and recommended its use nationwide. The Charter describes the rights of patients and other people using the Australian health system. The ultimate aim is to ensure that wherever and whenever care is provided, it is of a high quality and it is safe.

The Charter sets out seven rights of service users, one of which is the right to privacy. Service users have a right to privacy and confidentiality of their personal information. According to the Charter[82] this means that personal privacy is maintained and the proper handling of personal health and other information is assured.

The Commission has produced a number of guidance documents relating to the Charter and how it is to be used, aimed at patients, carers, families, healthcare providers and healthcare staff.

The Commission has also produced a poster asking patients and service users: "Do you know your healthcare rights?" The poster encourages service users to ask their providers for brochures or fliers about the Charter and to contact the Commission for further information.

State Departments of Health have developed codes and guidance for health professionals based on legislation and the key concepts outlined in this section.

5.7 Provisions at state level

5.7.1 South Australia

5.7.1.1 South Australia *Code of Fair Information Practice*[83]

The Department of Health has adopted a Code of Fair Information Practice to ensure that all public hospitals and health units comply with a set of Privacy Principles. The Code was developed in response to a growing community concern, identified by the Department, regarding privacy when providing personal information to any organisation and the recognition that it is important that consumers have confidence that the Department will handle their personal information in a fair, secure and appropriate manner.

The principles of the Code regulate the way in which information is collected, used, disclosed, stored and transferred. In respect of the appropriate secondary use of health information the following are the key principles[83]:

- Ensure that the person concerned knows why you are collecting information and what you will do with it
- Use and disclose information only for the purpose for which it was collected (primary purpose)
- Seek consent from the individual prior to using or disclosing their information for purposes other than the primary purpose. If this is neither practicable nor possible, ensure that the Code permits the use or disclosure
- Enable clients to exercise the option of remaining anonymous where this is lawful and practicable
- Implement security and privacy measures when transferring information to others.

5.7.1.2 Privacy Committee of South Australia

The Government of South Australia has issued an administrative instruction requiring its government agencies to generally comply with a set of information privacy principles and has established a Privacy Committee to oversee compliance. The Privacy Committee oversees the application of the Information Privacy Principles by State Government agencies, reports to the Minister and provides advice on privacy issues. The principal officer of each agency is required to ensure the Information Privacy Principles are implemented, maintained and observed in respect of the personal information they collect and hold.

5.7.1.3 *Your Rights and Responsibilities – A Charter for Consumers of the South Australian Public Health System*[84]

Your Rights and Responsibilities – A Charter for Consumers of the South Australian Public Health System[84] provides general information about consumers' rights in respect of the health services they access. This includes rights to information, consent to treatment, confidentiality of information and the right to receive appropriate care.

5.7.2 Victoria

5.7.2.1 Relevant Legislation

There are two key pieces of legislation for consideration in Victoria – the Information Privacy Act 2000[85] and the Health Records Act 2001[86]. The Information Privacy Act[85] sets standards for how Victorian government organisations, the State public sector, statutory bodies and local councils collect and handle personal information.

However, the definition of personal information within the Act does not extend to health information or personal information collected by a health service provider in order to provide a health service. Information privacy is covered in the provisions of the Health Records Act 2001[86], which is regulated by the Health Services Commissioner[****].

The Health Records Act 2001 protects health information handled by the Victorian public and private sectors. The Act established standards called Health Privacy Principles (HPP) for the collection, handling and disposal of health information in the public and private sectors. One of the aims of the Act is to balance the public interest in protecting the privacy of health information with the public interest in its legitimate use[87]. This is the key concept in the appropriate secondary use of health information.

5.7.2.2 The Health Privacy Principles

The standards set by the Health Records Act are contained in eleven Health Privacy Principles (HPPs) and a contravention of any of these is viewed as "an interference with the privacy of an individual"[87].

Principles one, two and eight are most relevant to governing the secondary use of information. Principle one requires that organisations notify individuals about what they intend to do with the information collected. Principle two relates to use and disclosure. It states that organisations must only use or disclose health information for the primary purpose for which it was collected or a directly related secondary purpose the person would reasonably expect[87].

Otherwise, consent is generally required. Principle eight, anonymity, is also relevant. It requires organisations to give individuals the option of not identifying themselves when entering transactions with organisations where this is lawful and practicable[87]. This allows for the information to be used for secondary purposes, such as research, without risk to the patient's privacy or identity.

5.7.2.3 The Health Services Commissioner

The Commissioner is responsible for implementing the provisions of the Health Records Act[86] and handling complaints made about an interference with health privacy. A complaint can be made against any person or organisation that collects, holds or discloses health information.

[****] The Office of the Health Services Commissioner (HSC) is an independent statutory authority established to receive and resolve complaints about health services. The HSC also handles complaints about disclosures of health information and access to health information. A complaint can be made against any person or organisation that collects, holds or discloses health information.

The role also includes educating organisations that collect and handle health information about their obligations under the Act, as well as educating Victorians about their rights[87]. The Commissioner has produced a number of information sheets for service users and providers outlining rights and responsibilities in respect of the Health Records Act. These are available on the Health Services Commissioner's website http://www.health.vic.gov.au/hsc/.

5.8 Summary

The governance of health information privacy in Australia is beset by a patchwork of codes of practice, guidelines and statutory requirements that vary at federal and state level and also between the public and private healthcare sectors.

There have, however, been moves in recent times towards developing a more structured and cohesive approach – primarily in the form of proposed amendments to the Privacy Act. In 2006 the Australian Government commissioned a review of the Privacy Act by the Australian Law Reform Commission, which published its recommendations in 2008. At the time of writing this document the proposals and discussions are ongoing.

In the interim the following developments and initiatives have taken place in respect of the secondary use of information in Australia:

- In 2010 Draft Australian Privacy Principles were published, which if incorporated into the new Act will replace the Information Privacy Principles and the National Privacy Principles that are currently in place. It is anticipated that this will bring Australia significantly closer to achieving the aim of national consistency both across the public and private sectors and also across Commonwealth, state and territory jurisdictions.

- The existing privacy principles require that the individual is well informed of why their information is being collected and the purposes it will be used for. They also place limits on the use of personal information and the conditions that must be satisfied in order to use information for a secondary purpose.

- One of the recommendations by the ALRC is to enhance and clarify the protections around the sharing of information and the ability to use information to facilitate research in the public interest - a document due to be published by the government for public consideration outlining specific privacy protections for information relating to health is pending release at the time of writing this report.

- The Royal Australian College of General Practitioners has produced guidance on the use of information in private medical practice. The importance of open communication with patients is a key point. The guidance explores the steps to be taken when proposing to use information for secondary purposes and outlines the process when the use is for teaching purposes, for research and for quality assurance and continuing professional development, highlighting that there are differences within the types of secondary uses that can take place.

- Provisions in place at a state level echo the secondary use principles in the existing information and national privacy principles. This is primarily that service users are informed of how their information will be used and it will not be used for another purpose unless the individual has consented to the use.

6. Conclusion

Health information is undoubtedly a valuable resource, the use of which can bring many benefits in terms of improving the quality and safety of care and developments in research. However, this needs to take place in an environment that is respectful to the rights of service users in terms of protecting their privacy and confidentiality and the right to be in control of how their information is used.

With the appropriate safeguards in place, which facilitate a greater trust in healthcare professionals, service users are more likely to be willing to share their information and allow for it to be used for purposes not directly related to their treatment or care. Clear guidelines need to be in place in terms of what uses are appropriate and what conditions need to be satisfied in order to use information for a secondary purpose.

This international review is the first step in determining those guiding principles that will form part of the IG guidance being developed by the Authority.

6.1 Summary of Findings

Of the information that was sourced in the course of this review the following are the key points:

Increased need for guidance on the secondary use of information:

One of the findings of the review was that there is a consensus regarding the need for guidance around the secondary use of information. Legislative provisions concerning the secondary use of information are typically contained within general privacy or data protection legislation.

Guidance and codes of practice have typically centred on privacy and confidentiality with the appropriate secondary use of information being covered as an aspect within it. More recently guidance is emerging that focuses solely on how information can be used and disclosed – focusing on what secondary uses are appropriate.

Examples include the British Medical Association's document *How to respond to requests for disclosure of data for secondary purposes*[4], the College of Physicians and Surgeons of Alberta's *Framework for the secondary use of health information*[5] and in Australia the *Handbook for the Management of Health Information in Private Medical Practice*[6].

Informing and involving the service users in decisions about their information:

The key recommendation in the guidance documents explored as part of this review was the need to be open and transparent with service users about the uses of their information. The importance of informing and engaging with service users about how their information may be used is reiterated in guidance documents and codes of practice that were sourced in each of the countries explored.

A number of the guidance documents emphasise the ways in which this can be done, for example posters and leaflets in waiting rooms outlining the ways in which information may be used and the reasons for it. One example as documented in the Australian *Handbook for the Management of Health Information in Private Medical Practice*[6] is the use of information for quality assurance purposes.

Patients should be made aware that their information may be used for this purpose and have the benefits of the practice clearly explained to them. A recurring message can be identified in the literature which asks health professionals if a patient would be surprised to learn that their information was being used in this way – if so they are not being effectively informed.

Differentiation between types of secondary use:

One of the findings in the course of the review is that clear distinctions are drawn between different secondary uses of health information, for example use for teaching purposes, quality assurance purposes such as clinical audit and research purposes. However, the categorisation of clinical audit in itself is not clearly defined, for example in England it is seen to be a primary healthcare function where the audit is carried out internally by the NHS organisation but a secondary use of the information if it requires disclosure to an external auditor.

In the guidance explored different steps are outlined which must be followed depending on the type of use. The *NHS Code of Practice on Confidentiality*[7] presents a model outlining three different types of disclosure – for healthcare purposes (which includes clinical audit when conducted internally), medical purposes other than healthcare for example disclosure to cancer registries, and non-medical purposes for example to a hospital chaplain.

The National Ethics Advisory Committee in New Zealand has produced ethical guidelines for observational research[8] which base their requirements for ethical review on the principle that the intensity of ethical scrutiny should be proportionate to the level of risk of the activity.

Consent:

The review identified consent as a key concept to be addressed in the context of the secondary use of health information. At the most basic level of interpretation, consent must be obtained for the collection, use or disclosure of information for purposes outside the direct provision of care.

However, there are caveats to this - based on the type of secondary use as depicted above, whether consent needs to be explicit or whether implied consent will suffice (for example by information patients that their information may be used for local clinical audit through leaflets or posters in a waiting room) and steps that can be taken where it is not possible to gain consent.

The conditions that must be satisfied vary between countries depending on legislative requirements and in some cases bodies have been established specifically to provide guidance and advice in this area for example the Ethics and Confidentiality Committee in England.

The approval of research ethics committees and their requirements are also central to the ability to proceed without the consent of the individuals concerned. Despite the variations between rules and provisions internationally the optimum position in all cases is to obtain consent.

Anonymisation:

One of the findings of the review is the recommendation that where possible information should be anonymised before it is used for secondary purposes. In Ireland, once information has been anonymised the provisions of the Data Protection Acts cease to apply as the information is no longer identifiable.

The legislative provisions are similar internationally but questions have been raised around the definition of the term anonymised. For example can information be said to be anonymised if the process is reversible? Irrevocable anonymisation of personal data puts it outside data protection requirements in Ireland as it can no longer be linked to an individual. Guidance recommends that for all secondary uses information should be anonymised at the earliest point possible in the process. Typically, where anonymised information is being used consent is not required but best practice suggests that patients should still be informed.

Data Sharing Agreements:

One of the findings of the review is that data sharing agreements offer an additional safeguard against inappropriate use of information once it has been disclosed to a person or body outside the organisation (data controller). Typically, they require the body receiving the information to adhere to the same principles that the data controller does in respecting the privacy, confidentiality and security of the information.

The IG toolkit in the UK requires that secondary use organisations agree protocols governing the routine sharing of personal information with other organisations. Legislation within Canadian provinces is increasingly dictating the need for the Canadian Institute for Health Information (CIHI) to enter into data sharing agreements with third party data recipients. CIHI also undertakes audits of third party data recipients to ensure that they meet their contractual obligations.

6.2 Next Steps

Using the information sourced in this review, the next step in this programme of work is to identify the themes and principles that can be appropriately tailored to the Irish health and social care context. This will inform the development of detailed IG guidance, which will assist providers in complying with the forthcoming *National Standards for Safer Better Healthcare* and also act as a general resource for all health and social care professionals.

References

(1) The Department of Health and Children. *The National Health Information Strategy*. 2004. Available online from: http://www.dohc.ie.

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

(3) The Health Information and Quality Authority. *Guidance on Privacy Impact Assessment in Health and Social Care*. 2010.

(4) The Ethics Department, British Medical Association. *How to respond to requests for disclosure of data for secondary purposes*. 2011.

(5) College of Physicians and Surgeons of Alberta. *Data Stewardship: Secondary Use of Health Information*. 2009.

(6) The Royal Australian College of General Practitioners. *Handbook for the Management of Health Information in Private Medical Practice*. 2002.

(7) The Department of Health, UK. *Confidentiality: NHS Code of Practice*. 2003.

(8) The National Ethics Advisory Committee, New Zealand. *Ethical Guidelines for Observational Studies: Observational research, audit and related activities*. 2006.

(9) The Health Information and Quality Authority. *International Review of Information Governance Structures*. 2009. Available online from: http://www.hiqa.ie.

(10) The Health Information and Quality Authority. *An "As Is" Analysis of Information Governance in Health and Social Care Settings in Ireland*. 2010. Available online from: http://www.hiqa.ie.

(11) Comber, H., Director of the National Cancer Registry of Ireland. *Secondary Use of Data - Striking a Balance.* In: *Promoting Health Research and Protecting Patient Rights.* 29 November 2006. 2006. Available online from: http://www.dataprotection.ie.

(12) The Office of the Data Protection Commissioner. *Data Protection Guidelines on Research in the Health Sector*. 2007. Available online from: http://www.dataprotection.ie.

(13) The Office of the Data Protection Commissioner. *Ninth Annual Report of the Data Protection Commissioner*. 1997. Available online from: http://www.dataprotection.ie.

(14) Parliamentary Office of Science and Technology, UK. *Data Protection and Medical Research*. Report No.: 325. 2005.

(15) The General Medical Council, UK. *Confidentiality guidance: Disclosing information with consent* [Online]. Available from: http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality_24_35_disclosing_information_with_consent.asp. Accessed on: 19 October 2011.

(16) Health and Social Care Act, UK. 2001.

(17) Health and Social Care Act, UK. 2008.

(18) National Health Service Act, UK. 2006.

(19) The National Information Governance Board for Health and Social Care. *Ethics and Confidentiality Committee*. 2011.

(20) The Department of Health, UK. *The Patient Information Advisory Group (PIAG)* [Online]. Available from: http://www.dh.gov.uk/ab/Archive/PIAG/index.htm. Accessed on: 19 July 2011.

(21) The Department of Health, UK. *Confidentiality: NHS Code of Practice - supplementary guidance: public interest disclosures*. 2010.

(22) The Department of Health UK. *Research Governance Framework for Health and Social Care*. 2005.

(23) The Information Commissioner's Office, UK. *Use and Disclosure of Health Data - guidance on the application of the Data Protection Act, 1998*. 2002.

(24) The Data Protection Act, UK. 1998.

(25) The Information Commissioner's Office, UK. *About the Information Commissioner's Office* [Online]. Available from: http://www.ico.gov.uk/about_us.aspx. Accessed on: 12 August 2011.

(26) Medical Act, UK. 1983.

(27) The General Medical Council, UK. *General Medical Council - Regulating doctors, ensuring good medical practice* [Online]. Available from: http://www.gmc-uk.org/about/index.asp. Accessed on: 12 August 2011.

(28) The General Medical Council, UK. *Confidentiality*. 2009.

(29) The Ethics Department, British Medical Association. *Guidance on secondary uses of patient information*. 2007.

(30) The British Medical Association. *Confidentiality and disclosure of health information toolkit*. 2009.

(31) The Department of Health, UK. *Information Security Management: NHS Code of Practice*. 2007.

(32) NHS Connecting for Health. *Information Governance Toolkit* [Online]. Available from: https://www.igt.connectingforhealth.nhs.uk/. Accessed on: 20 October 2011.

(33) NHS Connecting for Health. *Information Governance Toolkit Secondary Use Organisation Version 9 (2011-2012)* [Online]. Available from: https://www.igt.connectingforhealth.nhs.uk/RequirementsList.aspx?tk=408344733370081&lnv=2&cb=89be5d06-679b-4d1d-add0-5157f4b07043&sViewOrgType=19&sDesc=Secondary Use Organisation. Accessed on: 20 October 2011.

(34) The Department of Health, UK. *A Question of Balance: Independent Assurance of Information Governance Returns - Summary of Guidance*. 2010.

(35) Canada Health Act. 1984.

(36) Canadian Institutes of Health Research. *Secondary Use of Personal Information in Health Research: Case Studies*. 2002.

(37) Quebec Charter of Human Rights and Freedoms. 2009.

(38) Canada Health Infoway. *White Paper on Information Governance of the Interoperable Electronic Health Record (EHR)*. 2007.

(39) The Organisation for Economic Cooperation and Development. *OECD Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Available online from: http://www.oecd.org.

(40) The Canadian Standards Association. *Model Code for the Protection of Personal Health Information*. 1996.

(41) Personal Information Protection and Electronic Documents Act (PIPEDA), Canada. 2000.

(42) Privacy Act, Canada. 1985.

(43) Office of the Privacy Commissioner of Canada. *Privacy Legislation in Canada* [Online]. Available from: http://www.priv.gc.ca/fs-fi/02_05_d_15_e.cfm. Accessed on: 29 January 2010.

(44) The Newfoundland and Labrador Centre for Health Information. *Privacy, Confidentiality and Access Principles and Guidelines for the Health Information Network* [Online]. Available from: http://www.nlchi.nf.ca/pdf/principles_guidelines_revised2004.pdf. Accessed on: 17 February 2010.

(45) Canadian Institute for Health Information. *Privacy and Security Framework*. 2010.

(46) Canadian Institute for Health Information. *Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-identified Data*. 2010.

(47) Canadian Institute for Health Information. *A Year in Review: CIHI's 2009-2010 Annual Privacy Report*. 2010.

(48) Canadian Institute for Health Information. *Privacy and Data Protection*. 2010.

(49) Personal Health Information Protection Act, Ontario. 2004.

(50) Advisory Committee on Information and Emerging Technologies (ACIET). *Pan-Canadian Health Information Privacy and Confidentiality Framework* [Online]. Available from: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php. Accessed on: 21 August 2009.

(51) College of Physicians and Surgeons of Alberta Medical Informatics Committee. *Data Stewardship Framework*. 2006.

(52) John Wilson. *Government and Nation - System of Government* [Online]. Available from: http://www.teara.govt.nz/en/government-and-nation/4. Accessed on: 25 January 2010.

(53) New Zealand Ministry of Health. *New Zealand's Health and Disability System* [Online]. Available from: http://www.moh.govt.nz/healthsystem. Accessed on: 25 January 2010.

(54) The Wave Advisory Board to the Director-General of Health. *From Strategy to Reality: the WAVE Project*. 2001.

(55) Health Information Strategy Steering Committee, New Zealand. *Health Information Strategy for New Zealand* [Online]. Available from: http://www.moh.govt.nz/moh.nsf/0/1912064EEFEC8EBCCC2570430003DAD1/$File/health-information-strategy.pdf. Accessed on: 29 September 2009.

(56) The Health and Disability Commissioner NZ. *The Code of Health and Disability Services Consumers' Rights*. 1996.

(57) Health and Disability Commissioner Act, New Zealand. 1994.

(58) Whiddet, R., Hunter, I., Engelbrecht, J. and Handy, J. Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics.* 2006; 75 pp.530-41.

(59) Hunter, I.M., Whiddett, R.J., Norris, A.C., McDonald, B.W., and Waldon, J.A. New Zealanders' attitudes towards access to their electronic health records: preliminary results from a study using vignettes. *Health Informatics Journal.* 2009; 15(3): pp.212-28.

(60) Palliative Care Council of New Zealand. *Sharing Patient Health Information: a review of health information privacy and electronic health records in New Zealand*. 2010.

(61) The Office of the Privacy Commissioner, New Zealand. *The Health Information Privacy Code 1994 - Revised Edition*. 2008.

(62) The Office of the Privacy Commissioner, New Zealand. *On the Record: A Practical Guide to Health Information Privacy*. 2011.

(63) The Office of the Privacy Commissioner, New Zealand. *Health Information Privacy Fact Sheet 1: Overview*. 2011.

(64) The Office of the Privacy Commissioner, New Zealand. *Health Information Privacy Fact Sheet 2: Collection of health information*. 2011.

(65) The Office of the Privacy Commissioner, New Zealand. *Health Information Privacy Fact Sheet 3: Disclosure of health information - the basics*. 2011.

(66) The Privacy Act, New Zealand. 1993.

(67) The Department of Health and Children. *Audit of Key International Instruments, National Law and Guidelines Relating to Health Information for Ireland and Selected Other Countries*. 2008.

(68) The Privacy Commissioner, New Zealand. *The Privacy Act and Codes* [Online]. Available from: http://privacy.org.nz/the-privacy-act-and-codes/. Accessed on: 19 October 2011.

(69) The Office of the Privacy Commissioner, New Zealand. *The Office of the Privacy Commissioner of New Zealand - About Us* [Online]. Available from: http://privacy.org.nz/introduction/. Accessed on: 26 September 2011.

(70) The Office of the Privacy Commissioner, New Zealand. *Health-related privacy case notes* [Online]. Available from: http://privacy.org.nz/health-privacy-toolkit/?highlight=health privacy toolkit.

(71) National Ethics Advisory Committee. *National Ethics Advisory Committee (NEAC)* [Online]. Available from: http://www.neac.health.govt.nz/. Accessed on: 20 October 2011.

(72) Australian Health Ministers' Advisory Council (AHMAC). *National Health Information Agreement Australia* [Online]. Available from: http://www.health.gov.au/internet/main/publishing.nsf/content/9DDCE2BA01AFDB12CA2571EA000E165E/$File/psyap6.pdf.

(73) Sahukar, N. , Acting Deputy Director, Policy Office of the Privacy Commissioner. *In: Federal Health Privacy Law and Options for Reform.* In: *Medico Legal Congress 2008.* 27 February 2008. 2008. Available online from: http://www.privacy.gov.au/materials/types/speeches/view/6286.

(74) Privacy Act, Australia. 1988.

(75) Privacy Amendment (Private Sector) Act, Australia. 2000.

(76) Health Records and Information Privacy Act, New South Wales. 2002.

(77) Office of the New South Wales Privacy Commissioner. *Health Records and Information Privacy Act 2002 - Statutory guidelines* [Online]. Available from: http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/pages/PNSW_03_hripact#4b.

(78) The Australian Law Reform Commission. *The Australian Law Reform Commission - About Us* [Online]. Available from: http://www.alrc.gov.au/. Accessed on: 29 September 2011.

(79) The Australian Law Reform Commission. *For Your Information: Australian Privacy Law and Practice*. 2008.

(80) Australian Government. *Australian Privacy Principles Companion Guide*. 2010.

(81) Office of the Privacy Commissioner, Australia. *Public Sector Information Sheet - Information Privacy Principles*. 2008.

(82) The Australian Commission on Safety and Quality in Health Care. *The Australian Charter of Healthcare Rights*. 2008.

(83) Department of Health, Government of South Australia. *South Australia Code of Fair Information Practice*. 2006.

(84) South Australia Department of Health. *Your Rights and Responsibilities - A Charter for Consumers of the South Australian Public Health System*. 2011.

(85) Information Privacy Act, Victoria. 2000.

(86) Victorian Health Records Act. 2001.

(87) Office of the Health Services Commissioner, Victoria. *Health Privacy - it's my business*. 2002.

Published by the Health Information and Quality Authority

For further information please contact:

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

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