Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

International Review of Information Security in Health and Social Care

July 2012

Safer Better Care

About the Health Information and Quality Authority

The Health Information and Quality Authority (HIQA) is the independent Authority established to drive continuous improvement in Ireland's health and personal social care services, monitor the safety and quality of these services and promote person-centred care for the benefit of the public.

The Authority's mandate to date extends across the quality and safety of the public, private (within its social care function) and voluntary sectors. Reporting to the Minister for Health and the Minister for Children and Youth Affairs, 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 those health and social care services in Ireland that by law are required to be regulated by the Authority.

- **Social Services Inspectorate** – Registering and inspecting residential centres for dependent people and inspecting children detention schools, foster care services and child protection services.

- **Monitoring Healthcare Quality and Safety** – Monitoring the quality and safety of health and personal social care services and investigating as necessary serious concerns about the health and welfare of people who use these services.

- **Health Technology Assessment** – Ensuring the best outcome for people who use our health services and best use of resources by evaluating the clinical and cost effectiveness of drugs, equipment, diagnostic techniques and health promotion activities.

- **Health Information** – Advising on the efficient and secure collection and sharing of health information, evaluating information resources and publishing information about the delivery and performance of Ireland's health and social care services.

Overview of the Health Information function

Health is information-intensive, generating huge volumes of data every day. It is estimated that up to 30% of the total healthcare 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, health and social care 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 appropriate treatment may be delayed or not given. In a children's residential centre, family access arrangements need to be communicated and recorded to inform a child's care plan.

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

Under section (8)(1)(k) of 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 service user 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. It can help identify trends in notifiable incidents in nursing homes.

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 users being asked to provide the same information on multiple occasions.

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

individuals are being encouraged to take more responsibility for their own health and well-being, yet it can be very difficult to find consistent, understandable and trustworthy information on which to base their decisions.

As a result of these deficiencies, there is a clear and pressing need to develop a coherent and integrated approach to health information, based on standards and international best practice. A robust health information environment will allow all stakeholders – the general public, patients and service users, health and social care professionals and policy makers – to make choices or decisions based on the best available information. This is a fundamental requirement for a highly reliable health and social care 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 guidance for information governance in Ireland. In order to inform the development of guidance, international reviews of the component parts of information governance are required. They are information governance management, data quality, information security, privacy and confidentiality and secondary use of information. Information security forms an integral component of information governance and is the subject of this international review.

Table of Contents

Executive Summary

1. Background

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

Information governance 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.[(2)] Good information governance is essential to ensuring an appropriate balance between using personal health information 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, 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 security of personal health information is a component of this.

Health information security can be defined as the protection of information from a wide range of threats in order to ensure continuity of care, minimise risk, and maximise the availability of required information in order to provide safe, effective care.[(4)]

Health information, whether in paper or electronic format, is vital to the provision of safe care to service users and to the business processes of health and social care organisations. Consequently, it is vital that health information is suitably protected. This is especially important in the increasingly interconnected health and social care environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

2. International Review

An initial desktop review of health information security and its key principles in health and social care identified four countries for further examination. Due to language constraints it was necessary to select English-speaking countries. The countries were chosen based on information security initiatives and resources identified in the desktop review, the availability of information and the fact that initiatives and reform in this area are ongoing in each of these jurisdictions. As such, the information

presented is current and up to date and the initiatives deal with issues of relevance to the area. The review examines the following countries:

- England
- Canada
- New Zealand
- Australia.

A brief overview of international standards and of the current situation in Ireland is also given in the introductory section of the document.

3. Findings

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

- Information security

  Information security or data security is a recognised information governance topic in all countries reviewed. Although it is not acknowledged in its own right in federal health legislation in Canada and Australia, its principles and associated practices are a strong focus in their information governance strategies and policies.

- Legislation, standards, policies and procedures

  Guidance documents, policies and strategies in the countries reviewed discuss information security mainly as a facet of privacy or information governance in general. Requirements in this area are set out. However, there are no formal national standards with the exception of those within the information governance toolkit in England. Information security policies and procedures have been developed at a provider level based on national guidance and codes of practice in England and New Zealand, for example *Information Security Management: NHS Code of Practice* [5] in England and as part of the *Health Information Privacy Code 1994*[6] in New Zealand. There is recognition in Canada and Australia of the need for federal legislation and standards for information security that are applicable to all organisations across territories and the public/private divide as a definitive resource for requirements. There is scope for providers in Canada and Australia to build on policies developed by organisations such as the Canadian Institute for Health Information's (CIHI) *Privacy and Security Framework*[7] and the National E-Health Transition Authority's (NEHTA) *E-Health Information Security and Access Framework*[8] in Australia , as these are based on legislation. It is likely that this will happen in the coming years as both Canada and Australia are actively working towards a more national approach to information governance.

- Support and guidance

An oversight body provides guidance and support in the form of information brochures and guidelines for information security, such as *Health Information Privacy Factsheet 5: Storage, Security, Retention and Disposal of Health Information* produced by the Office of the Privacy Commissioner in New Zealand to assist organisations in meeting the legislative requirements of the *Health Information Privacy Code*.[9] In all countries reviewed, this oversight body is responsible for the enforcement of the country's privacy or data protection legislation. With regard to the above example, in New Zealand the Office of the Privacy Commissioner has responsibility for ensuring compliance with the *Health Information Privacy Code*.[6]

- Information security plan

In each of the countries explored, the importance of developing a plan for information security is highlighted whether at national policy level or provincial level. This is echoed and likely influenced by the International Organisation for Standardisation (ISO) standards reviewed. The information security plan should detail the types of information collected, stored and shared by the organisation and a comprehensive risk assessment to highlight areas for improvement in information security practices.

- Assessment and compliance

Self-assessment of compliance with national (where available) and local codes of practice and guidelines is a recurring theme in each of the countries, particularly in the information governance toolkit in England. Self-assessment is also discussed in the international resources included in this review, such as in the International Organisation for Standardisation (ISO) standard *ISO/IEC 27001: 2005, Information technology - Security techniques - Information security management systems – Requirements*.[10] This emphasises the need to continuously monitor progress in this area and develop improvement plans as appropriate.

- Ehealth initiatives

In each of the countries reviewed, it appears that a major driver for the development and implementation of robust national rules around health information security is the advancement of ehealth initiatives such as electronic health records. This is due mainly to the increased levels of information sharing afforded by ehealth initiatives and the associated increase in information security risk that occurs. For example, NEHTA's *E-Health Information Security and Access Framework*[8] was specifically introduced for this reason.

- Training and education

  The importance of educating staff about information security practices and providing ongoing training is evident in each of the reviewed countries, particularly in England where it is required as a part of the information governance toolkit.

4. Next steps

Prior to commencing the development of information governance guidance, the Authority sought to inform itself through this review of the international experience. Having completed this review, the next step for the Authority is to identify the overarching themes within the review and areas to be covered under the umbrella of information security to inform the development of information governance guidance.

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 respect of health information this also includes ensuring that service users' interests are appropriately protected. This includes the right to privacy, confidentiality and security of their personal information which form part of information governance.

The Authority is currently working towards developing guidance for information governance 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[11] and an As Is Analysis of Information Governance in Health and Social Care Settings in Ireland.[12] In the course of these reports the following topics were identified as the core aspects of information governance:

- information governance 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 information governance framework. Information governance is also covered at a high level as a standard in the *National Standards for Safer Better Healthcare*[13] launched by the Authority in 2012 following mandating by the Minister for Health. The 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 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 information governance guidance. This guidance will assist providers in complying with the national standards and also act as a general resource for all health and social care professionals.

1.2 What is health information security?

Health information security can be defined as the protection of information from a wide range of threats in order to ensure continuity of care, minimise risk, and maximise the availability of required information in order to provide safe, effective care.[4]

Health information, whether in paper or electronic format, is vital to the provision of safe care to service users and to the business processes of health and social care

organisations. Consequently, it is vital that health information is suitably protected. This is especially important in the increasingly interconnected health and social care environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Health information exists in many media and can be required for different purposes. In health and social care, it may be printed or written on paper files, stored electronically, transmitted by post or by using electronic means or messaging, conveyed using television media, or spoken in conversation between health and social care professionals and service users. It is important that health information is appropriately protected in all forms and means by which it is shared or stored.

Health information security can be achieved by implementing appropriate policies, procedures, processes, organisational structures and software and hardware functions. This helps to ensure the physical and electronic protection of information both stored, in use and in transit in such a manner that it is only accessible to those who require access and are fully authorised. Robust health information security can prevent against loss, unauthorised amendment and destruction of information. Information security controls should be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the objectives and requirements of health and social care organisations are met.[4;10]

1.3 Legislation and Guidance

This review aims to aid the development of guidance in relation to the protection of personal health information while facilitating access by service providers as and when required in the provision of patient care. There are legislative provisions outlining the information security measures to be taken by service providers that collect, store, use and share health information. It is anticipated that the forthcoming Health Information Bill will include further provisions in respect of personal health information security.

1.3.1 The legislation

The Data Protection Acts 1988[14] and 2003[15] (the Acts) place an obligation on data controllers to have appropriate security measures in place to prevent accidental loss, unauthorised access to, or unauthorised amendment, disclosure or destruction of the data. There must also be processes in place to protect against the accidental loss or destruction of data. Data controllers and data processors are also obliged to ensure that their staff and other persons in the workplace are aware of security measures and comply with them. The legal obligation to keep personal data secure applies to every data controller and data processor, regardless of size.

The Acts do not detail specific security measures that a data controller or data processor must have in place. Rather, Section 2(1)(d) places an obligation on

persons to have appropriate measures in place to prevent 'unauthorised' access to, or alteration, destruction or disclosure of, the data and against their accidental loss or destruction. The amended Act in 2003 clarified the nature of security measures required to demonstrate compliance with Section 2(1)(d). When determining security measures, a number of factors need to be taken into account:[16]

- the state of technological development
- the cost of implementing measures
- the harm that might result from unauthorised or unlawful processing
- the nature of the data concerned.[16]

A further development introduced by the 2003 Act is the obligation on data controllers and data processors to ensure that their staff are aware of security measures and comply with them. In line with this, in 2008 the Office of the Data Protection Commissioner made available guidelines that are intended as an indication of issues which data controllers and data processors should consider when developing security policies.

The Data Protection Guidelines for Developing Security Policies[16] advises that the following topics are addressed when developing a security policy:

- access control
- encryption
- anti-virus software
- firewalls
- automatic screen savers
- logs and audit trails
- the human factor
- certification
- remote access
- wireless networks
- portable devices
- back-up systems.

1.3.2 Guidance developed by the Authority to date

In 2011, the Authority issued a guidance booklet entitled *What you should know about Information Governance, A Guide for health and social care staff*.[17] The booklet provides a broad overview of information governance issues as they relate to personal health information in the Irish health and social care setting. The guidance emphasises that by improving the security of patient and service-user information through robust security processes, controls and management that the confidentiality of personal information can be maintained.[17]

In 2010 the Authority issued guidance[3] together with a self-assessment tool 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 expand a dataset of personal health information or to share health information. 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 completed sample PIA for assistance and a self-assessment tool to allow organisations to identify and evaluate potential privacy and security risks. A PIA, when conducted properly, will identify any actual or potential privacy and information security concerns associated with a proposed project and allow the identification of appropriate information security measures. The guidance is intended as a resource for all those involved in healthcare delivery, project planning and research.(3)

The Authority is currently working towards developing detailed guidance for information governance for the Irish health and social care sector. The purpose of this international review, together with reviews undertaken on the other aspects of information governance, namely information governance management, data quality, privacy and confidentiality and secondary use of information is to inform the development of the detailed guidance for information governance. This guidance will assist providers in complying with the national standards and also act as a general resource for all health and social care professionals.

1.4 International Review

Along with a review of international information security standards, the countries that are reviewed in detail in this report are England, Canada, New Zealand and Australia. The countries were chosen based on the results of a desktop review that identified a range of initiatives that could contribute to developing detailed information governance guidance for health and social care in Ireland, particularly with respect to information security. The developments documented in each of the countries are recent and in some cases are ongoing at the time of writing ensuring that the information that will inform the detailed information governance guidance is as current and up to date as possible.

A review of standards from the International Organisation for Standardisation (ISO) relevant to health information security is also included in this international review as these standards heavily influence the policy on information security in the countries reviewed.

2. International Standards

ISO (the International Organisation for Standardisation) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardisation. National bodies that are members of ISO or IEC participate in the

development of International Standards through technical committees established by the respective organisation to deal with particular fields of activity.

2.1 ISO/IEC 17799: 2005

ISO standard *ISO/IEC 17799: 2005, Information technology — Security techniques — Code of practice for information security management* has been developed to establish guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation. The standard provides guidance on defining information security, why information security is necessary, assessing information security requirements and developing a robust information security policy based on risk assessment under a number of heading areas.(4)

The approach for addressing information security in the standard emphasises the following topics:

- risk assessment
- development of a security policy
- organising information security requirements
- physical and environmental security
- security of employee personal information
- access controls to personal information
- information system security and asset management
- compliance with legal requirements
- information security incident management.(4)

2.2 ISO/IEC 27001: 2005

ISO standard *ISO/IEC 27001: 2005, Information technology — Security techniques — Information security management systems – Requirements* has been developed to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS).(10)

The process approach for information security management presented in the standard emphasises the importance of:

- understanding an organisation's information security requirements and the need to establish policy objectives for information security
- implementing and operating controls to manage an organisation's information security risks in the context of the organisation's overall business risks
- monitoring and reviewing the performance and effectiveness of the ISMS
- continual improvement based on objective measurement.(10)

The influence of these international standards on international health information policies, codes of practice, standards and frameworks is evident in the international review that follows.

3. England

3.1 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 from national taxation. In England, responsibility for the NHS is devolved to 10 strategic health authorities (SHAs), 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 (PCT) are responsible for providing primary and community services and for commissioning secondary care services for 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.[11] There is a structured approach to information governance in England at a national and local level.

3.2 Health information security in England

The NHS is a rich source of health information facilitating the delivery of health and social care and 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.

A number of developments have taken place in an attempt to safeguard the security of personal health information. Each of the following serves to protect the health information of service users:

- legislation
- Department of Health
- NHS Connecting for Health.

3.3 Legislation

The Data Protection Act 1998[18] contains eight data protection principles. Principle 7 details the legal requirements of The Data Protection Act under information security.[19] In particular, organisations must:

- design and organise security to fit the nature of the personal data held and the harm that may result from a security breach

- be clear about who in the organisation is responsible for ensuring information security

- make sure the right physical and technical security is in place, backed up by robust policies and procedures and reliable, well-trained staff

- be ready to respond to any breach of security swiftly and effectively.[19]

The Patient Information Advisory Group (PIAG) was established under the Health and Social Care Act 2001[20] 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.[21] One of the functions of the NIGB is to oversee arrangements created under Section 251 of the National Health Service Act 2006.[22] Section 251 allows identifiable patient information to be used for research purposes where it can be demonstrated that access to identifiable patient data is necessary and that the research cannot be carried out using de-identified data. This represents a high risk to the information security of individuals involved.[23] As well as a review by the committee, all section 251 applications undergo a security review to ensure that the security measures in place are compliant with those required to process patient identifiable information. A system-level security policy template is provided to applicants to ensure that all relevant detail is provided.[24]

3.4 Department of Health

3.4.1 Code of Practice on Information Security

In 2007 the Department of Health published a code of practice for the NHS on information security.[5] The code of practice was developed by a working group of relevant stakeholders and wide consultation was undertaken with providers. The document provides a guide to standards of practice and methods concerning information security for those who work within or under contract to NHS organisations. The code of practice is an integral component within the information security management framework and the overall NHS information governance programme. Information security is defined in the code as: "The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved."[5]

The code of practice is based on current legal requirements in England, relevant standards and professional best practice with the purpose of identifying and addressing security management in the processing and use of health information. The types of information covered by the code include paper and digital healthcare

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

records, administrative information, medical images and reports, emails, financial records and health information held on mobile devices.

The code of practice presents a model of the core elements of an effective information security management system (ISMS). These are:

- Plan – establish the ISMS
    - define the need for information security and detail this in a corporate information security policy
    - identify and assess risks to information security
    - identify how information security risks can be mitigated or controlled.
- Do – implement and operate the ISMS
    - develop and implement plans to manage identified information security risks
    - develop and implement information security training for all staff.
- Check – monitor and review the ISMS
    - establish processes to discover and document information security breaches
    - monitor and update information security risk assessments regularly
    - monitor the effectiveness of the ISMS by internal reviews and independent audit at regular intervals.
- Act – improve and maintain the ISMS
    - review and update the ISMS as appropriate.[5]

This model is adapted from ISO/IEC 17799:2005 and provides for establishing, implementing, operating, monitoring and improving the effectiveness of information security management in an NHS organisation.

3.4.2 Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents

In 2010, the Department of Health published a checklist for reporting, managing and investigating information governance serious untoward incidents (SUIs).[25] An information governance SUI is defined in the checklist as any incident involving the actual or potential loss of personal information that could lead to identity fraud or have other significant impact on individuals. This checklist forms an important part of the information security policy developed by the Department of Health in England for the NHS. The checklist details a systematic process for evaluating, reporting, investigating and managing potential SUI occurrences in the form of a set of questions which guide the provider to the appropriate actions.

The key purposes of the checklist are to ensure:

- a consistent approach to evaluation and management of information governance SUI's across the NHS
- appropriate preventative action is taken with regard to SUIs
- appropriate action is taken in the event of an SUI
- lessons learned are identified and communicated.

The main components of the management process in the checklist include initial reporting, managing the incident, investigation and final reporting. These components detail how to assess the severity of a SUI and the reporting rules necessary; for example, a serious information security breach involving more than 1,000 personally identifiable health records must be reported to the Department of Health and the Information Commissioner in England.[25] The checklist must be used to assess near misses and should aid organisations in developing incident response plans appropriate to the type of information held.

3.4.3 Critical National Infrastructure Protection Programme

Information systems used by NHS organisations are becoming increasingly interconnected. This creates many new and useful benefits, but at the same time, these arrangements introduce new risk factors. Many of the critical services that are essential to the delivery of health and social care are dependent on information and communication technology. These services are provided by both public and private sector organisations. The government is identifying the core services that need to be secured from electronic attack and is seeking to work with those organisations responsible for these systems so that these services are protected in a way that is proportional to the threat. This is known as the Critical National Infrastructure (CNI) protection programme and information systems used by NHS organisations have been identified as part of the CNI.[26]

The National Infrastructure Security Co-ordination Centre (NISCC) was established in 1999 by the Home Secretary with the purpose of coordinating and developing existing work within public and private sector departments, agencies and organisations to defend the CNI against electronic attack. In 2005, the NISCC was succeeded by the Centre for the Protection of Infrastructure (CPNI). The CPNI is responsible for coordinating:[27]

- identification of the most critical CNI systems and working with organisations to reach a level of assurance about the protection of those systems
- alerts or warnings of attacks
- assistance in response to serious attacks
- information about identified threats
- specialist protective information security advice and expertise.[26;27]

The NHS systems are a crucial part of the CNI; therefore NHS information systems and networks must be appropriately managed and protected from security

threats.[26] NHS Connecting for Health helps organisations and service providers to identify risks, implement preventative measures and respond to security breaches that may result in adverse events. NHS Connecting for Health works with the CPNI to ensure the effectiveness of these measures and to aid the development of organisational awareness of information security.

The Unified Incident Reporting and Alert Scheme (UNIRAS) is the English government's computer emergency response team and is operated by the CPNI. It gains support from the Communications-Electronic Security Group (CESG), which is the national technical security authority of the United Kingdom.[27] UNIRAS gathers reports of significant electronic security attacks, threats and preventative measures from organisations within the CNI group and disseminates them back to the entire group in the form of security alerts and information briefings. Many NHS security advice notices are based on reports received from UNIRAS.[26]

3.5 NHS Connecting for Health

NHS Connecting for Health (CfH) forms part of the health informatics directorate in the Department of Health. The role of CfH is to develop and maintain the NHS national IT infrastructure with the primary aim of helping to improve patient care and safety.[28] CfH put forward three principles of effective health information security:

- confidentiality – health information must be secured against unauthorised access
- integrity – health information must be safeguarded against unauthorised modification
- availability – health information must be accessible to users when it is required.[29]

The NHS CfH also provides security incident management advice for organisations to use when managing information security issues. One of these requirements is that all service providers develop and implement a detailed security incident management plan. This requirement is based on recommended practice in ISO 27001[30]. Essentially, each provider must provide a roadmap indicating clearly the steps to be taken when things go wrong, such as a breach of information security resulting in the loss of health information.

3.5.1 Information Governance Toolkit

The Information Governance Toolkit (IGT)[1] is a web-based application, hosted by NHS CfH, and designed to facilitate organisations to self-assess the way they handle or process information. The toolkit enables organisations to measure their compliance with a range of information governance related legislation and requirements including the Data Protection Act,[18] the International Information Security Standard: ISO/IEC 27001:2005[4] and the NHS Code of Practice on Information Security Management.[5]

The toolkit is reviewed and updated annually and version 10 was released in July 2012. The toolkit consists of information governance requirements that are subdivided into six work areas:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance.[1]

The information security assurance work area is further divided into a number of requirements tailored to different types of organisation related to health and social care. Each requirement contains guidance to assist providers in compliance and also exemplar materials as resources.[1] The requirements refer in the main to ensuring robust and appropriate policies, procedures and processes are developed and implemented by staff who possess adequate skills, knowledge and experience to satisfy each organisations' obligations in relation to information security. The requirements include that policies and procedures must be in place for:

- organisational obligations as a registration authority. A registration authority is an organisation with responsibility for managing the registration and updating of NHS health records and staff access to NHS health records
- incident reporting and management of incidents
- ensuring networks operate securely
- business continuity in the event of an information security breach, equipment failure, environmental hazard or human error and subsequent temporary loss of an information asset
- ensuring computer components are capable of detecting, isolating and removing malicious code
- secure operation of mobile and tele-working
- use of pseudonyms and/or anonymized data to protect the confidentiality of service users wherever possible
- management of staff access rights to personal and sensitive information
- risk assessment of information security weaknesses, such as during the transfer of personal information between systems or locations.[1]

Requirements to meet information security needs include:

- a senior risk owner should be accountable for risk policy and strategy within each organisation
- staff training on information security is provided and updated regularly
- process monitoring to ensure compliance with information security requirements
- maintenance of a comprehensive information asset register detailing software, hardware and information services within the organisation
- regular review and update of the information security risk assessment.[1]

Each requirement has four attainment levels, level 0 through to level 3, with level 0 being entirely non-compliant with the requirement. The attainment levels are cumulative and it is not possible to achieve level 3 without already satisfying all components of levels 1 and 2. There are criteria for satisfying each requirement attainment level and evidence of compliance examples given to aid the organisation in achieving each level. For example:

Attainment-level evidence of compliance example – Information Governance Toolkit

Requirement 9-302: There are documented information security incident/event reporting and management procedures that are accessible to all staff.

Level 0 – There is insufficient evidence available to attain level 1.

Level 1 – There are documented and approved processes for reporting, investigating and managing information security incidents / events.

The following criteria must **all** be satisfied:

a. There are documented procedures for reporting, investigating and managing information security events, including confidentiality/data loss Serious Untoward Incidents (SUIs).

Evidence: documented reporting, investigating and managing information security events procedures.

b. The procedures have been approved by the Senior Information Risk Officer, and Board or delegated sub-group involving IAOs or equivalent personnel.

Evidence: information governance Management Framework document (which includes the date the procedures were approved and the approving individual/group).[(1)]

The toolkit has continued to evolve and change annually in response to a changing information governance 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 information governance responsibilities. It enables service providers to identify areas where their performance is poor and demonstrates the ways in which improvements can be made.

Audits of information governance 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 information governance toolkit self-assessments in 2010.[31] The audit framework aims to help NHS organisations to 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.

3.6 Summary

The approach to health information governance, and specifically information security as a part of this, is highly structured at a national level. Legislation in the form of the Data Protection Act 1998 provides the legal basis for information security under Principle 7. The Code of Practice for Information Security produced by the NHS provides the basis for information security in health and social care with detailed standards based on the code developed by NHS Connecting for Health in the form of the information governance Toolkit. This affords health and social care organisations and professionals a strong degree of certainty about their obligations in terms of protecting health information.

The following are key developments of note in relation to health information security in England, outlining information security requirements and providing guidance at a national level across the health sector:

- NHS Code of Practice on Information Security[5]
- Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents[25]
- Critical National Infrastructure Protection Programme[26]
- NHS Connecting for Health Information Governance Toolkit and audits of self-assessments against the toolkit.[1;31]

4. Canada

4.1 Introduction

Canada's population of approximately 34 million people is governed as a parliamentary democracy consisting of a federation of 10 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.(32)

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

4.2 Health information security in Canada

A number of initiatives and developments are in place at a pan-Canadian level to safeguard health information security as a part of privacy and general information governance initiatives. These include:

- Legislation
- Canadian Institute for Health Information (CIHI) guidance
- The Pan-Canadian Health Information Privacy and Confidentiality Framework
- Canada Health Infoway.

4.3 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.(33) 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(34) 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.(35) This Code has been formally incorporated as Schedule 1 of the Personal Information Protection and

Electronic Documents Act (PIPEDA)[36]. PIPEDA applies to both federal and provincial entities.

Canada has two federal privacy laws: the Privacy Act[37] and the Personal Information Protection and Electronic Documents Act (PIPEDA)[36]. 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 personal health information. It gives individuals the right to access, and request correction of, personal information about themselves held by these organisations.[36] PIPEDA confers these obligations on private sector organisations. Principle 7 of PIPEDA maintains that an organisation is required to employ adequate security safeguards to protect personal information. As the information becomes more sensitive, the level of security required increases. An organisation that establishes safeguards but fails to follow them violates the Act. Appropriate safeguards should include:

- physical measures, for example, locking filing cabinets and restricting access to offices
- organisational measures, for example, security clearances and limiting access to a 'need-to-know' basis
- technological measures, for example, the use of passwords and encryption.[36]

4.4 The Canadian Institute for Health Information

The Canadian Institute for Health Information (CIHI) is an independent, not-for-profit organisation that provides data and analyses of the Canadian health system and the health of Canadians.[38] CIHI has offices in Ottawa, Toronto, Montreal, Edmonton and Victoria and performs analyses of health information and data received from hospitals, regional health authorities, medical practitioners and governments. Although not involved in the provision of clinical care, CIHI analyses a large volume of patient identifiable health information, which presents a challenge in terms of ensuring that this information is properly protected.

4.4.1 Comprehensive privacy and security policies

CIHI maintains a comprehensive privacy and security 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[7] and Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data, 2010.[39] Although these policies have been developed specifically by CIHI they are aligned with the federal Personal

Information Protection and Electronic Documents Act (PIPEDA).[40] As such they could be used as a basis for other organisations developing a suite of information governance policies and procedures, particularly in relation to provisions around information security.

One of the key commitments in the privacy and security framework integral to the work of CIHI is the privacy and security of data. At the core of this commitment is recognition that information is only secure if it is secure throughout its entire lifecycle of creation and collection, access, retention and storage, use, disclosure and disposition. Accordingly, CIHI has implemented administrative, technical and physical safeguards to protect personal health information under its control. A comprehensive suite of policies, and associated standards, guidelines and procedures reflect best practices in privacy, information security and records management for the protection of the confidentiality, integrity and availability of CIHI's information assets.[41]

4.4.2 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 and in the Personal Health Information Act in Newfoundland and Labrador.[42] CIHI's prescribed entity status in legislation enables it to collect personal health information in those provinces without patient consent. However, the legislation also provides for strict security safeguards that CIHI must adhere to with respect to the personal health information collected, for example, a requirement to ensure all staff who handle health information are sufficiently trained in information security practices. In response to this requirement, CIHI developed a privacy and security education and awareness programme for staff and designated September of each year as information security awareness month with regular staff education sessions held.[39]

4.5 Pan-Canadian Health Information Privacy and Confidentiality Framework

In an attempt to harmonise existing Canadian privacy and security 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 known as the ACIET Framework.[43] The ACIET Framework provides guidelines for common and consistent statutory provisions for the collection, use and disclosure of personal health information. The framework applies to both the public

[¥] 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 utilisation of emerging health products and technologies to the Conference of Federal, Provincial, and Territorial (F/P/T) Deputy Ministers of Health.

and private healthcare sectors and although it is a guide rather than a standard, it serves as a tool for regulators as they seek to develop consistent privacy and security requirements through the introduction or amendment of health privacy legislation.(43)

Custodians and trustees of electronic health records must establish and implement audit, security, and availability safeguards. Audit, security and availability safeguards to address reasonably anticipated security risks in the electronic environment include:

- data encryption
- access controls
- routine audit trails
- use of privacy enhancing technologies
- secured back-up and recovery of records
- business resumption planning
- disaster recovery planning
- general availability of information communication technologies, for example, during power outages.(43)

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 inform and influence the development and review of health privacy statutes in Canada.

4.6 Canada Health Infoway

Canada Health Infoway (Infoway), is a not-for-profit federally funded organisation that collaborates with the provinces and territories, healthcare providers and technology solution providers to accelerate the use of electronic health records (EHRs) in Canada. Each province is responsible for the development of its own EHR system. However, Infoway provides a technology blueprint, vendor certification and standards to foster interoperability and best practice across the provinces and territories.(44) In 2007, Infoway developed and published a *White Paper on Information Governance of the Interoperable Electronic Health Record (iEHR).*(45) This document discusses the issues surrounding rules, requirements and mechanisms involved in handling personal health information including the security of personal health information. It also provides the basis for discussion by key stakeholders to deal with their jurisdictional approaches to information governance. Specific to information security, the white paper discusses access controls, information security incident management, audit of information security practices and the use of electronic digital signatures as a security strengthening tool.

In order to successfully introduce a pan-Canadian iEHR, Canada Health Infoway recognises that provincial and territorial approaches to information governance must be cohesive. Infoway works closely with the jurisdictions to integrate privacy into the interoperable EHR and to identify and leverage best practices for re-use across the country. Infoway's Electronic Health Record Solution (EHRS) Blueprint includes a

privacy and security architecture component which ensures the sharing of personal health information is secure at all points of transfer.[46]

The Privacy Forum established in 2007 and sponsored by Infoway, includes representatives from each federal, provincial and territorial Ministry of Health and privacy oversight body. The Forum offers a mechanism for members to share and leverage their collective knowledge and experience on privacy and security matters in the development of interoperable iEHR initiatives. Infoway also sponsors the Health Information Privacy (HIP) Group. Established in 2008, this group made up of health ministry representatives, is focused on the consideration of common approaches to information governance issues pertinent to privacy and security in electronic health information systems.[46]

Infoway Certification Services review EHR solutions to determine whether the product conforms to assessment criteria. Privacy and security are key components of this certification.[46]

4.7 Summary

Although many territorial and provincial rules exist around information security, there appears to be recognition that a move towards a pan-Canadian approach through legislation and initiatives from organisations such as Canada Health Infoway will foster a more cohesive and safe information security environment in health. This is particularly important with advances in information technology leading to higher adoption of ehealth initiatives such as the electronic health record and increased sharing of healthcare records.

The following are key developments of note in relation to health information security in Canada:

- Canada has two federal privacy laws encompassing information security: the Privacy Act[37] and the Personal Information Protection and Electronic Documents Act (PIPEDA)[36]
- the Privacy and Security Framework[7] developed by CIHI and aligned with the PIPEDA
- the Pan-Canadian Health Information Privacy and Confidentiality Framework known as the ACIET Framework[43] developed by a collaboration of provincial deputy health ministers
- the Privacy Forum and Health Information Privacy group established by Canada Health Infoway.

5. New Zealand

5.1 Introduction

New Zealand has a population of approximately 4 million people and is governed by a parliamentary democracy system. The government is fully integrated nationally with no separate states or territories.[47] 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.[48] 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 and governance structures. The *Working to Add Value through E-information (WAVE) Report – From Strategy to Reality*[48] 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.[49]

At the time of writing this report the New Zealand health agenda is very much focused towards e-health. Health information security is coming increasingly to the fore as the country moves closer to the widespread use of electronic health records.

5.2 Health information security in New Zealand

There are a number of resources available to service providers and service users which build upon each other and convey the themes and issues relevant to ensuring health information is securely held and processed:

- Legislation
- the Health Information Privacy Code
- guidance issued by the Office of the Privacy Commissioner.

5.3 Legislation

Legislatively, it is the Privacy Act 1993[50] which is of primary importance in New Zealand. The Privacy Act sets out 12 information privacy principles on collecting, using, keeping, disclosing, transferring, accessing and securing personal information.[51] The provisions of the Privacy Act are administered by the Privacy Commissioner.

Principle 5 of the Privacy Act relates to information security. It states that any agency collecting, using or disclosing personal information must ensure:

- that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, access, use, modification, or disclosure, except with the authority of the agency that holds the information

- that if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.[50]

The Privacy Act made provision that any code of practice based on the Act developed by the Privacy Commissioner for a specific sector, would become lawful.[50] One such code is the Health Information Privacy Code 1994[6], which was revised in 2008. This means that the rules contained within the Health Information Privacy Code[6] 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.

5.4 The Health Information Privacy Code 1994

The Health Information Privacy Code 1994,[6] 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 12 information privacy principles in the Privacy Act.[50] It expands on the information privacy principles in the Privacy Act and applies the rules specifically in the context of 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.

Rule 5 of the Health Information Privacy code relates to storage and security of health information. It states that appropriate security arrangements must be in place to address:

- physical security, for example, physically securing and restricting access to the areas where health information is stored

- user operational security, for example, requiring as part of an employment contract or contract of service that all employees collecting, using or disclosing health information comply with the code

- system operational security, for example, developing rules on levels of access and taking steps to ensure that access to different categories of information is available only to authorised users

- technical security, for example validating software used for recording, processing, storing and retrieving health information through detailed audit, and certifying software as suitable for appropriate use

- security of transmission, for example, using unique identifiers, rather than names, to ensure electronic and manual transmission of confidential information about individuals is secure

- disposal or destruction of health information, for example, physical records may be destroyed by controlled incineration, ensuring that individual records are not lost or removed during the process and that the resulting waste does not include fragments of readable personal information.

The code also recommends that all organisations develop a security plan detailing firstly, a classification of all the health information collected and stored by the organisation to allow an understanding of the sensitivity of the information assets held. A risk assessment highlighting potential information security risks should then be undertaken and procedures put in place to manage the identified risks. The code recommends that ISO 27001: 2006 provides guidance on the objectives of strong information security. 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.

5.5 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 powers including investigating complaints about breaches of privacy and examining proposed legislation and the impact it may have on individual privacy.[52]

With respect to the security of health information the Privacy Commissioner has produced a number of documents and resources that offer guidance to health and social care professionals. In May 2011 the Privacy Commissioner launched a health privacy toolkit aimed at health consumers and health providers.[52] 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[6]
- a series of health information privacy fact sheets[9]
- *On the Record: A Practical Guide to Health Information Privacy*[53]
- Health related privacy case notes (summaries of health related privacy complaints).[54]

5.5.1 Health Information Privacy Fact Sheets

The Office of the Privacy Commissioner has produced a series of five fact sheets relating to the health information privacy code, which 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.

Health Information Privacy Factsheet 5: Storage, Security, Retention and Disposal of Health Information provides guidance to health professionals on their obligations with regard to health information security.[9] The factsheet particularly focuses on rule 5 of the Health Information Privacy Code, explaining each requirement and providing examples on how to identify information security risks, develop and implement an information security plan and where to find additional guidance.[9]

5.5.2 *On the Record: A Practical Guide to Health Information Privacy*

The Office of the Privacy Commissioner has produced *On the Record: A Practical Guide to Health Information Privacy* as a ready reference guide for managing common situations that people in the healthcare organisations face. This guide incorporates information security processes as a method to safeguard the privacy of individuals. It uses examples to illustrate the legislative requirements and gives advice on developing policies. The aim of the guide is to give practical advice that can be applied easily within the workplace.[53]

The guide provides real world examples of information security risks and breaches occurring and explains how these could be mitigated within the confines of the Health Information Privacy Code. It is intended to be utilised alongside relevant legislation such as the Privacy Act and recommends further that all staff are provided with training on information security and privacy law and the Health Information Privacy Code.[53]

5.6 Summary

The following are key points to note in relation to health information security in New Zealand.

New Zealand has robust legislation in the form of the Privacy Act 1993 and the Health Information Privacy Code 1994 (revised 2008), which govern the security of health information nationally. The Office of the Privacy Commissioner is responsible for enforcing this legislation and has produced a number of guides to help healthcare organisations in fulfilling their obligations in terms of information governance and specifically health information security. Relevant guides produced to date are

available to health professions in a single location in the form of the Health Privacy Toolkit which includes:

- the Health Information Privacy Code[6]
- a series of health information privacy fact sheets[9]
- *On the Record: A Practical Guide to Health Information Privacy*[53]
- Health related privacy case notes (summaries of health related privacy complaints).[54]

As in other countries reviewed, health information security is viewed in New Zealand as a component of information governance that is strongly related to privacy, in that it is a tool that facilitates the privacy of individuals.

6. Australia

6.1 Introduction

Australia operates a federal system of government in which power is divided between the Commonwealth Government and 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 10 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. 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, public health, research and national health information management. Each state and territory has individual responsibility for the management and delivery of public health services and the regulation of healthcare practitioners within their state or territory boundary.(55)

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).(56) The latest version of this agreement came into effect in September 2004.

6.2 Health information security in Australia

The basis for governing health information security 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. Privacy principles which include an information security component 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 safeguarding privacy and maintaining security of information in general. The governance structure and the types of health and social care organisations the legislation applies to have been the cause of further confusion as principles and sources of guidance are further divided in terms of the public and private sector. In 2010 the Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner and their functions were combined in order to foster more cohesion in the area of information privacy and security. Integration work is ongoing at the time of writing of this report.(57)

Health information security will be discussed in the context of:

- legislation
- health information security in private medical practice
- the National e-Health Transition Authority
- Standards Australia eHealth.

6.3 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.(56) 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.(56) The integration of the Office of the Privacy Commissioner and the Office of the Australian Information Commissioner served in part to address this issue and was underpinned in legislation in 2010 in the form of the Australian Information Commissioner Act 2010.(57)

Legislation will be discussed under the following headings:

- federal legislation
- state legislation
- legislative reform.

6.3.1 Federal legislation

The relevant federal legislation for health information security is the Privacy Act 1988.(58) The Privacy Act has regulated the handling of personal information held by all federal government agencies and by 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 with the exception of the Australian Capital Territory which is covered by the Federal Privacy Act.(59)

Health information is classified as sensitive information in the Privacy Act which as a result, provides for extra protections around the handling of personal health information. The Act governs information security requirements along with other aspects of privacy for the organisations under its remit.(58)

The Privacy Act 1988 consists of two sets of privacy principles, Information Privacy Principles and National Privacy Principles. The former set of principles applies to the government and public sector agencies while the latter applies to the private sector.

Principles 4 of both the Information Privacy Principles and the National Privacy Principles relate to information security and are very similar.[58]

Principle 4 of the Information Privacy Principles states that a record keeper who has possession or control of a record that contains personal information shall ensure:

- that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse

- that everything reasonably within the power of the record keeper is done to prevent unauthorised use or disclosure of information contained in the record.[58]

Principle 4 of the National Privacy Principles states that:

- an organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure

- an organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.[58]

There appears to be no rationale for maintaining this dual approach to the privacy principles within a single piece of legislation and calls have been made to develop a unified set of privacy principles for a more consistent national approach to privacy regulation.

6.3.2 State legislation

In Australia, 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. One example is the Health Records Act 2001 (HRA) in Victoria.[60] 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 Victoria. Principle 4 of the HRA relates to data security and data retention and states that:

- an organisation must take reasonable steps to protect the health information it holds from misuse and loss and from unauthorised access, modification or disclosure

- a health service provider who deletes health information in accordance with this Act must make a written note of the name of the individual to whom the health information related, the period covered by it and the date on which it was deleted

- a health service provider who transfers health information to another individual or organisation and does not continue to hold a record of that information must

make a written note of the name and address of the individual or organisation to whom it was transferred

- an organisation other than a health service provider must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected.[60]

6.3.3 Legislative reform

The Australian Law Reform Commission (ALRC)[#] promotes national consistency in relation to the privacy of personal health information. In 2008 the ALRC published *For Your Information: Australian Privacy Law and Practices.*[62] 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 security of health information, the following are the key recommendations:[62]

- develop a single set of privacy principles to replace the Information Privacy Principles and the National Privacy Privacy Principles
- enhance and clarify the protections around the sharing of health information.

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[63] and it is anticipated that they will form a key part of the amendments to the Privacy Act.

The release of the Draft Australian Privacy Principles[63] marked the first step in the Australian government's 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.

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

[#] 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.[61] 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.[61]

cohesion both across the public and private sectors and also across Commonwealth, state and territory jurisdictions.[64]

6.4 Health information security in private medical practice

In line with the provisions of the Privacy Act,[58] 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*[*].[65] 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, confidentiality and security of personal health information.

Section 8 of the handbook advises GPs on data security and retention, expanding on the National Privacy Principles and providing an appendix which details guidance on secure storage and transfer of health information.[65]

6.5 The National E-Health Transition Authority

The National E-Health Transition Authority (NEHTA) was established by the Australian state and territorial governments to develop better ways of electronically collecting and securely exchanging health information.[66]

In December 2011, NEHTA launched a *National eHealth Information Security and Access Framework* (NESAF) with the purpose of increasing the certainty among individuals that health information is created and accessed in a secure and trustworthy manner.[8] The goals of information security in the framework are confidentiality, availability and integrity of health information. These goals are achievable through use of information security measures such as the development of an information security policy, use of authorised access controls, audit of information-handling processes and provider accountability for information security practices. The framework was influenced by federal legislation but was developed in recognition of the disparate health information security legislation at federal and territorial level in Australia.[8]

6.6 Standards Australia eHealth

Standards Australia is currently developing information security standards for ehealth in Australia as part of its health informatics work programme.[67] A working group of stakeholders with wide expertise in healthcare and information technology are

[*] 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.

currently reviewing international information security standards such as ISO 27001 and new developments internationally with regard to health information security in order to inform the development of national standards for information security for ehealth in Australia.[67]

6.7 Summary

The governance of health information security in Australia is highly fragmented with numerous 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 but also in the form of national initiatives by NEHTA and Standards Australia eHealth.

In 2006 the Australian Government commissioned a review of the Privacy Act by the Australian Law Reform Commission, which published its recommendations in 2008. These recommendations included the development of new overarching privacy principles applicable across the public and private sectors at both federal and state level. At the time of writing this document the proposal on the development of new privacy principles has been accepted by government but is not yet incorporated in the legislation.

The following are key developments of note in relation to health information security in Australia:

- *For Your Information: Australian Privacy Law and Practices*[62] published by the Australian Law Reform Commission
- the publication of Draft Australian Privacy Principles[63] as a first step in reforming privacy law in Australia
- the publication of the *Handbook for the Management of Health Information in Private Medical Practice*[65]
- *National eHealth Information Security and Access Framework* (NESAF) published by the National eHealth Transition Authority[8]
- the work of Standards Australia in developing national standards for information security in line with the International Organisation for Standardisation standards as part of its health informatics work programme.[67]

National organisations in Australia are developing and have produced some key initiatives on information security, notably the National ehealth security and access framework developed by NEHTA and the ongoing work by Standards Australia to develop national standards for information security. These initiatives together with a move to develop overarching privacy principles at legislative level serve to standardise information security practices across the health sector and tackle the issue of disparate standards and rules across the public and private healthcare divide.

7. Conclusion

7.1 Summary of Findings

The purpose of this document is to explore the experience internationally of health information security and its associated principles and practices. This review is the first step in the process of developing guidance for information governance for the health and social care sector in Ireland. Information security can be described as an important aspect of information governance that enables the safe collection, storage and sharing of health information operating effectively and efficiently as part of the culture of any health and social care organisation. The countries reviewed in detail were England, Canada, New Zealand and Australia including the exploration of additional resources that could be used internationally. Many of the key principles of information security are shared across international boundaries although fragmentation of information security resources across various territories remains an issue in some countries with the exception of England which has the most advanced and cohesive structure for information security of the reviewed countries.

7.2 Findings

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

- Information security

  Information security or data security is a recognised information governance topic, usually as a part of privacy in all countries reviewed. Although it is not acknowledged in its own right in federal health legislation in Canada and Australia, its principles and associated practices are a strong focus in their information governance strategies and policies.

- Legislation, standards, policies and procedures

  Guidance documents, policies and strategies in the countries reviewed discuss information security mainly as a facet of privacy or information governance in general. Requirements in this area are set out, however, there are no formal national standards with the exception of those within the information governance toolkit in England. Information security policies and procedures have been developed at a provider level based on national guidance and codes of practice in England and New Zealand, for example *Information Security Management: NHS Code of Practice*[5] in England and as part of the *Health Information Privacy Code 1994*[6] in New Zealand. There is recognition in Canada and Australia of the need for federal legislation and standards for information security that are applicable to all organisations across territories and the public/private divide as a definitive resource for requirements. There is scope for providers in Canada and Australia

to build on policies developed by organisations such as the *Privacy and Security Framework*[7] developed by the Canadian Institute for Health Information (CIHI) and the *E-Health Information Security and Access Framework*[8] developed by the National E-Health transition Authority (NEHTA) in Australia, as these are based on legislation. It is likely that this will happen in the coming years as both Canada and Australia are actively working towards a more national approach to information governance.

- Support and guidance

An oversight body, such as the Information or Privacy Commissioner, provides guidance and support in the form of information brochures and guidelines for information security, such as *Health Information Privacy Factsheet 5: Storage, Security, Retention and Disposal of Health Information* produced by the Office of the Privacy Commissioner in New Zealand to assist organisations in meeting the legislative requirements of the *Health Information Privacy Code.*[9] In all countries reviewed, this oversight body is responsible for the enforcement of the country's privacy or data protection legislation. With regard to the above example, in New Zealand the Office of the Privacy Commissioner has responsibility for ensuring compliance with the *Health Information Privacy Code.*[6]

- Information security Plan

In each of the countries explored, the importance of developing a plan for information security is highlighted whether at national policy level or provincial level. This is echoed and likely influenced by the ISO standards reviewed. The information security plan should detail the types of information collected, stored and shared by the organisation and a comprehensive risk assessment to highlight areas for improvement in information security practices.

- Assessment and Compliance

Self-assessment of compliance with national (where available) and local codes of practice and guidelines is a recurring theme in each of the countries, particularly in the information governance toolkit in England. Self-assessment is also discussed in the international resources included in this review, such as in the International Organisation for Standardisation (ISO) standard *ISO/IEC 27001: 2005, Information technology – Security techniques – Information security management systems – Requirements.*[10] This emphasises the need to continuously monitor progress in this area and develop improvement plans as appropriate.

- Ehealth initiatives

In each of the countries reviewed, it appears that a major driver for the development and implementation of robust national rules around health information security is the advancement of ehealth initiatives such as electronic health records. This is due mainly to the increased levels of information sharing

afforded by ehealth initiatives and the associated increase in information security risk that occurs. For example, the *E-Health Information Security and Access Framework*[8] developed by the National E-Health transition Authority (NEHTA) in Australia was specifically introduced for this reason.

- Training and Education

  The importance of educating staff about information security practices and providing ongoing training is evident in each of the reviewed countries, particularly in England where it is required as a part of the information governance Toolkit.

7.3 Next Steps

Prior to commencing the development of information governance guidance, the Authority sought to inform itself through this review of the international experience. Having completed this review, the next step for the Authority is to identify the overarching themes within the review and areas to be covered under the umbrella of information security to inform the development of information governance guidance.

References

(1) NHS Connecting for Health. *Information Governance Toolkit*. NHS Connecting for Health Website . 2011. Available online from: https://www.igt.connectingforhealth.nhs.uk/.

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

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

(4) International Standards Organisation. *Information technology-Security techniques-Code of practice for information security management*. ISO/IEC FDIS 17799:2005 (E). 2005.

(5) Department of Health / Digital Information Policy. *Information Security Management: NHS Code of Practice*.

(6) Health Information Privacy Code 1994 (Revised 2008). 1994.

(7) Canadian Institute for Health Information. *Privacy and Security Framework*. 2011.

(8) National eHealth Transition Authority. *NEHTA Releases eHealth Information Security and Access Framework*. 2011.

(9) The Office of the Privacy Commissioner. *Health Information Privacy Factsheet 5: Storage, Security, Retention and Disposal of Health Information*. 2012. New Zealand.

(10) International Standards Organisation. *Information Technology – Security techniques – Information Security Management Systems – Requirements.* ISO/IEC 27001:2005(E). 2005.

(11) The Health Information and Quality Authority. *International Review of Information Governance Structures*. 2009.

(12) The Health Information and Quality Authority. *An "As Is" Analysis of Information Governance in Health and Social Care Settings in Ireland*. 2010.

(13) The Health Information and Quality Authority. *National Standards for Safer Better Healthcare*. 2012.

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

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

(16) The Office of the Data Protection Commissioner. *Data Protection Guidelines for Developing Security Policies*. 2008.

(17) Health Information and Quality Authority. *What you should know about Information Governance, A Guide for health and social care staff*. 2011.

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

(19) Information Commissioners Office. *Information security (principle 7)*. 2012. Available online from: http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx.

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

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

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

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

(24) National Information Governance Advisory Board. *Section 251* [Online]. Available from: http://www.nigb.nhs.uk/. Accessed on: 7 February 2012.

(25) Department of Health. *Checklist for Reporting, Managing and Investigating Information Governance Serious Untoward Incidents*. 2010. Available online from: http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/@ps/documents/digitalasset/dh_111501.pdf. Accessed on: 2 February 2012.

(26) Department of Health. *NISCC and UNIRAS: protecting the NHS infrastructure*. 2011.

(27) Centre for the Protection of National Infrastructure. *About the Centre for the Protection of National Infrastructure*. 2011.

(28) NHS Connecting for Health. *NHS Connecting for Health Systems and Services*. 2012.

(29) NHS - Connecting for Health. *Principles of Information Security*. 2012.

(30) NHS - Connecting for Health. *Security Incident Management*. 2012.

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

(32) Canada Health Act 1985. 1985.

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

(34) The Organisation for Economic Cooperation and Development. *OECD Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data*. 1980.

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

(36) Personal Information Protection and Electronic Documents Act. 2000. Available online from: http://www.pipeda.info/a/s4-7.html.

(37) Privacy Act, Canada. 1985.

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

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

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

(41) Canadian Institute for Health Information. *The CIHI Data Quality Framework*. Ottawa, Ontario: CIHI; 2011. Available online from: http://secure.cihi.ca/cihiweb/products/cihi_ps_framework_March2011_en.pdf.

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

(43) 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.

(44) Canada Health Infoway. *About Canada Health Infoway*. 2010. Available online from: http://www.infoway-inforoute.ca/lang-en/about-infoway.

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

(46) Canada Health Infoway. *Privacy Mandate*. 2012.

(47) 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.

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

(49) Ministry of Health. *New Zealand Ministry of Health* [Online]. Available from: http://www.moh.govt.nz/moh.nsf.

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

(51) 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.

(52) The Office of the Privacy Commissioner NZ. *The Office of the Privacy Commissioner of New Zealand - About Us* [Online]. Available from: http://privacy.org.nz/introduction/.

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

(54) 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.

(55) The Health Information and Quality Authority. *International Review of Unique Health Identifiers for Individuals*. 2010.

(56) Sahukar NMLC2S. *Federal Health Privacy Law and options for Reform*. 2008.

(57) The Office of the Australian Information Commissioner. *Protecting Information Rights – Advancing Information Policy. About us.* 2012.

(58) Privacy Act, Australia. 1988.

(59) 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.

(60) Health Records Act 2001. 2001.

(61) The Australian Law Reform Commission. *The Australian Law Reform Commission - About Us* [Online]. Available from: http://www.alrc.gov.au/.

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

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

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

(65) Royal Australian College of General Practitioners and the Committee of Presidents of Medical Colleges. *Handbook for the Management of Health Information in Private Medical Practice*. 2002.

(66) National eHealth Transition Authority. *National eHealth Transistion Authority: About Us*. 2012. Available online from: http://www.nehta.gov.au/about-us.

(67) Standards Australia eHealth. *Standards Australia eHealth: Information Security*. 2012.

Published by the Health Information and Quality Authority.

For further information please contact:

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

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