International Review of Information Governance Structures

December 2009

About the Health Information and Quality Authority

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

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

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

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

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

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

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

Foreword

In the Information Society, there is an increasing awareness of the value of personal information. However it must be managed properly in order to protect those whose information it is, and in order to maximise the potential benefits to be obtained from the collection and utilisation of such information(1).

The development of national standards for health information governance (IG) is at the forefront of the Irish health information agenda. The objective of the current Health Service Reform Programme[1] is to deliver better patient care and safety. This means using information – in manual and electronic form- more effectively than previously to improve healthcare outcomes while ensuring that an individual's control over his or her personal health information is appropriately respected. This requires an examination of how the information is used, the areas where it could be better used and the safeguards needed to ensure appropriate protection(2). The Health Information and Quality Authority (the Authority) has a function to develop standards and to monitor against these in respect of health information. As such the Authority has a key role to play in developing and monitoring standards for IG for health and social care system in Ireland.

The need for an IG framework has been reiterated since it was first recommended in the 2001 *Health Strategy, Quality and Fairness – A Health System for You*(3) and the need for it has been further emphasised by the *National Health Information Strategy*, the 2008 *Report of the Commission on Patient Safety* (4) and the *Draft Health Information Bill*(5). The importance of IG in healthcare settings has been well documented but at present the system is fragmented and lacks a cohesive structure that will reap the benefits and provide the safeguards of a fully functioning system. At a basic level a framework for IG protects people's information and allows for high quality information to be used to improve patient safety, care and the health service generally.

The Department of Health and Children, the Authority and healthcare providers (public and private) all have a role to play in developing and implementing national standards for IG for the health and social care system. The Health Information Inter-Agency Group was established in April of 2008; its membership is comprised of representatives from the Department of Health and Children, the Authority and the Health Service Executive (HSE). One of the primary objectives of the group was to clarify the respective roles of each of the members. In relation to national standards for health IG the roles have been agreed as follows:

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

- The Department of Health and Children has responsibility for legislation in the form of the Health Information Bill[2]
- The Authority has responsibility for the development and monitoring of the standards, as per the Authority's functions in the Health Act
- The HSE has responsibility for the implementation of the approved standards

The Health Information and Quality Authority was established under the Health Act 2007 with the primary statutory role to promote safety and quality in the provision of health and personal social services for the benefit of the health and welfare of the public. One of the functions of the Authority as set out in the Health Act 2007 is[(6)]:

8._(1) *(k)* to set standards as the Authority considers appropriate for the Executive and service providers respecting data and information in relation to services and the health and welfare of the population;

8._(1) *(l)* to advise the Minister and the Executive as to the level of compliance by the Executive and service providers with the standards referred to in *paragraph (k)*;

These statutory functions provide the basis for the Authority to develop national standards for health IG and to establish a method to monitor compliance. Monitoring compliance is essential in order to foster a culture of continuous development and improvement.

Action 18 of the *National Health Information Strategy 2004* is the development of a framework for IG[(5)]. The report states within this action that a specialist function for IG will be established by the Authority. In line with this, and the provisions in the Health Act the development of such a framework has been identified as a priority for the Authority[(6)]. This work will be completed in line with the provisions of the Health Information Bill and informed by consultation with stakeholders.

The purpose of this document is to examine how other countries have approached IG for health and social care settings. The Authority will also document what IG structures, policies, guidelines exists in the Irish health and social care sector. This will inform the Authority on how best to approach the development and monitoring of national standards for IG in the Irish health and social care sector.

[2] As part of the Health Reform Programme, the Department of Health and Children is preparing new legislation on the collection, use, sharing, storage, disclosure and transfer of personal health information as well as ensuring that the privacy of such information is appropriately respected. This will take the form of the Health Information Bill, due to be enacted in 2010.

Table of Contents

Executive Summary **7**

1 Introduction **9**

2 England **11**

2.1 Overview 11

2.2 Legislation 12

2.3 National structures for information governance 13

2.4 Provider governance structures 17

2.5 Summary 20

3 Scotland **21**

3.1 Overview 21

3.2 Scottish Legislation 22

3.3 National structures for information governance 24

3.4 Provider structures for information governance 28

3.5 Summary 29

4 Canada **30**

4.1 Overview 30

4.2 Legislation 30

4.3 National structures for information governance 31

4.4 Provider structures for information governance 33

4.5 Summary 36

5 Australia **38**

5.1 Overview 38

5.2 Legislation 39

5.3 National structures for information governance 40

5.5 Summary 45

6 New Zealand **46**

6.1 Overview 46

6.2 Legislation 46

6.3 National structures for information governance 47

6.4 Provider structures for information governance 52

6.5 Summary 53

7 Sweden **54**

7.1 Overview 54

7.2 Legislation 55

7.3 National structures for information governance 55

7.4 Provider structures for information governance 59

7.5 Summary 59

8 Conclusions **60**

Appendices **62**

Appendix 1 62

Acronyms 62

Appendix 2 63

IG Toolkit Acute Hospital 'View', Sample Requirement 63

Reference List **64**

Executive Summary

1 Background

IG has been a recurring item on the Irish health agenda for the past number of years. It was first recommended in the 2001 Health Strategy, Quality and Fairness – A Health System for You and the need for a framework was further emphasised in the *National Health Information Strategy 2004* and the 2008 *Report of the Commission on Patient Safety – building a Culture of Patient Safety*. The area has received further attention more recently with the development of an IG framework being identified as one of the objectives of the forthcoming Health Information Bill.

National standards for health IG are required to provide a single reference point for the way in which information should be collected, processed and used. As per the provisions of the Health Act, the Authority has a key role to play. The Authority has a function to develop standards and to monitor compliance with them. Prior to commencing the development of national standards for health IG the Authority has sought to inform itself, through this review, of international best practice. The review also provides an opportunity to learn from instances where initiatives have not been successful and attempts are now being made to improve the initiatives. The review is the first step in a process that will inform the development of national standards for health IG.

2 International review

Following a desktop review of IG, initiatives a number of countries that have well defined structures at a local or national level were deemed appropriate for further research. These included the following:

- England
- Scotland
- Canada
- New Zealand
- Australia
- Sweden.

Within each of these countries the supporting legislation for IG was explored. The review also documents what has been developed, or in some cases is being developed, at both a national and a provider level.

A structured national approach is a feature in England, Scotland and to a lesser extent New Zealand. In Canada, Australia and Sweden it has been recognised that a national approach is more appropriate and efforts are being made to work towards this.

Legislatively, the main areas of focus are the county specific, or equivalents, of Data Protection or Freedom of Information Acts. Most recently progress has been made in Sweden in relation to legislative provisions for IG through the Patient Data Act 2008.

Clear lines of accountability for IG issues was a further recurring theme – for example Caldicott Guardians in England and Scotland and equivalent privacy officers in Canada.

Self-assessment and methods to monitor compliance against standards or compliance with legislation were identified most strongly in England and Scotland through the use of an IG toolkit. This is a web-based self-assessment tool that enables organisations to measure annually their compliance against a range of information handling requirements.

3 Findings

IG is seen as a national health priority in each of the countries reviewed. It is discussed in depth, with a series of recommendations identified, in national strategies in Australia, New Zealand and Sweden. Although much of the focus in each of these is on eHealth, the issues that arise are applicable to the governance of all forms of information.

The following common themes emerged as a result of the international review:

- a structured national approach to IG - England and Scotland have developed a structured national approach with the others working towards this
- clear lines of accountability for IG at a national and local level, such as Caldicott Guardians in each healthcare organisation in England and Scotland acting as the "conscience" of that organisation.
- a central authority or point of reference on IG issues, for example the National Information Governance Board in England
- national standards and codes of practice for IG based on legislation, typically data protection and freedom of information legislation
- more specific policies and procedures developed at a provider level based on legislation and national codes of practice
- self-assessment tools and external audit to monitor compliance, such as the IG toolkit in England and Scotland.

1 Introduction

According to the *National Health Information Strategy (2004)* IG refers to

"a strategic framework that brings coherence and transparency to information initiatives and which is responsive to the spectrum of issues and concerns of those involved. Issues such as information sharing, health surveillance, quality assurance, confidentiality, privacy records management, freedom of information and data protection are included"[(7)].

It allows organisations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively, in order to deliver the best possible care. Additionally it enables organisations to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records where and when needed, in particular to meet requests for information and to assist compliance with corporate governance standards[(8)].

The 2001 report by the Department of Health and Children – *Quality and Fairness: a Health System for You* specifies that the Department will publish a Health Information Bill which will aim to put health IG on a sound and robust footing and provide a clear legislative context for supporting health service processes while recognising the rights and duties of clients/patients, health professionals and health agencies[(3)]. This would provide a set of rules to ensure full and proper use of information while fully protecting the privacy of the individual.

National standards for health IG are required to bring together all the legal requirements, standards and best practice that apply to the handling and sharing of health information. National standards will provide a single consolidated reference point for IG issues and will inform providers of the level they need to reach in order to comply with IG requirements. They are increasingly essential with improved information and communication technology, an increased number of health information systems and increased expectations for healthcare providers to share information. There has also been an increased awareness of human rights and ethical and psychological considerations relating to consent and privacy, furthering the case for comprehensive and nationally cohesive standards for health IG for the Irish health service.

Standards for health IG will be a single consolidated reference point for all providers of healthcare to adhere to in relation to the handling and management of personal health information. The standards will cover the following areas:

- IG management
- confidentiality and data protection assurance
- information security assurance
- clinical information assurance/care records assurance

- secondary use assurance
- freedom of information assurance.

Internationally there is a growing body of expertise on IG. The aim of this document is to explore the international structures for IG to inform the Authority on a framework for IG in Ireland. Following a desktop review of international IG structures and initiatives, a number of countries were deemed appropriate for further research. This was based on the development stage of IG structures at local or national level within the selected countries, initiatives that have been put in place and the availability of information. This document reviews the legislation, national structures and local structures for IG in the selected countries. A brief description of the government structures in each of the countries is also included as this has in some cases impacted on IG developments. The review examines the following countries:

- England
- Scotland
- Canada
- Australia
- New Zealand
- Sweden.

2 England

2.1 Overview

The United Kingdom (UK) operates a parliamentary democracy. Although responsibility for certain issues have been devolved to Scotland, Wales and Northern Ireland, England is governed solely by the UK Parliament.

A review carried out by the Care Record Development Board (now the National Information Governance Board) in 2005 on the IG practices in the UK Department of Health and the wider National Health Service (NHS) commented on the absence of a single coordinating body which could be an authoritative source of advice or arbitration, where there was a disagreement about best practice. The review recommended that a National Information Governance Board covering both health and social care should be established[9]. The National Information Governance Board (NIGB) was established following this recommendation. The overall finding of the review was that although the Department of Health (UK) and the NHS were striving towards good IG practices the present arrangements needed to be strengthened. The report put forward a number of recommendations to facilitate this as follows[9]:

- the function of the Caldicott Guardian[3] for the Department of Health should pass to the new Deputy Chief Medical Officer thus creating a line of accountability and leadership from this office through the Caldicott Guardians in the NHS
- all organisations providing health and social care are required in addition to having a Caldicott Guardian, to have clear processes with their overall governance structure to ensure compliance, oversight and monitoring of IG within that organisation
- a clear job description and competencies are created for Caldicott Guardians and training, support and guidance is provided for Caldicott Guardians and IG committees
- a National Information Governance Board is created to cover both health and social care to provide oversight, develop and interpret best practice, promote consistency, arbitrate on the interpretation of policy, give advice on the interpretation of policy, give advice and build public confidence in the NHS Care Record Service (CRS)
- all bodies or organisations supplying services to the NHS CRS bring their registration authority and procedures under the oversight of their IG committee and that proper management of user-registration is seen as an IG issue.

[3] A Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing.

2.2 Legislation

A number of acts contain provisions relating to health IG in England. Of these, the Data Protection Act 1998[10] and the Freedom of Information Act 2000[11] are most significant. The Department of Health, UK, has developed codes of practice for the NHS that are primarily based on the provisions contained in these pieces of legislation. These in turn have informed the development of policies and procedures at a provider level.

2.2.1 The Data Protection Act 1998 (UK)

The Data Protection Act 1998[4][10] requires anyone who handles personal information to comply with a number of important principles. It also gives individuals rights over their personal information. It contains three key strands[12] dealing with:

- notification by a data controller to the Information Commissioner[5] (this is the process of informing the information commissioner that processing of personal data is being carried out within a particular organisation)
- compliance with the eight data protection principles (outlined below)
- observing the rights of data subjects.

The eight principles of data protection advocate fairness and openness in the processing of personal information, ensuring that personal information is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept for longer than is necessary
- processed in line with patient rights
- secure
- not transferred to other countries without adequate protection.

The third area covered by the UK Data Protection Act provides individuals with important rights, including the right to find out what personal information about them is held on computer and most paper records. Should an individual or organisation feel they are being denied access to personal information they are entitled to, or feel their information has not been handled according to the eight principles.

[4] The same Data Protection Act was also enacted in Scotland

[5] The UK Information Commissioner is responsible for policing the Freedom of Information Act 2000 (does not apply to bodies covered by Scottish legislation). The UK information Commissioner also has responsibility for the enforcement of the Data Protection Act 1998.

2.2.2 The Freedom of Information Act 2000, UK

The Freedom of Information (FOI) Act[11] lays down requirements for public bodies to keep and make information available on request. The main features of the UK FOI Act 2000 are[12]:

- a general right of access to recorded information held by public authorities, regardless of the age of the record/document
- a duty on every public authority to adopt and maintain a scheme that relates to the publication of information by the authority and is approved by the Information Commissioner.

The UK Freedom of Information Act does not apply to bodies covered by the Scottish Freedom of Information legislation, as will be outlined in section 3.2.2 of this document.

2.3 National structures for information governance

Overall, the English model demonstrates a very structured national approach with clear lines of responsibility and accountability for IG.

The following are the structures in place in England to oversee IG:

- The National Information Governance Board
- The Department of Health, UK
- NHS Connecting for Health Information Governance Programme Board
- Caldicott Guardian Council UK
- Trust/Organisations Information Governance Committee/Groups.

2.3.1 The National Information Governance Board

Following the review of IG in the Department of Health and NHS in 2005, the National Information Governance Board (NIGB) was established. The NIGB was created for health and social care to advise the UK Department of Health and Ministers, to provide oversight, to develop and interpret best practice, to promote consistency, to arbitrate on the interpretation of policy and give advice and build public confidence in the NHS Care Records Service. The NIGB was established to be an over-arching IG body in England.

The board is independent and its membership drawn from stakeholders including patients and the public, health and social care professionals, NHS and independent providers, regulators and researchers. Membership of the board comprises of ten lay members appointed by the appointments commission and representatives of key

stakeholder organisations. The UK Council of Caldicott Guardians is one of the 11 representative members of the Board. The others are the Allied Health Professions Federation; the British Medical Association; the Academy of Medical Sciences; the Royal College of Nursing; the Patient Information Advisory Group; the Association of Directors of Adult Social Services; the Local Government Association; the NHS Confederation; the Independent Healthcare Advisory Services; and the Academy of Medical Royal Colleges.

The following organisations are corresponding members: the Royal College of Midwives; the Medical Protection Society; the Foundation Trust Network; the Strategic Health Authority Chief Information Officers Council; the General Medical Council; the Medical Defence Union; the Information Standards Board for Health and Social Care; and NHS Employers.

In the context of the NIGB, IG is defined as:

"The structures, policies and practice used to ensure the confidentiality and security of health and social care services records, especially clinical records, and to enable the ethical use of them for the benefit of the individual to whom they relate and for the public good."

The NIGB's terms of reference[13] are to:

- provide leadership and promote consistent standards for IG across health and social care, to enable ethical, legal and policy issues to be appropriately dealt with
- monitor IG trends and issues through analysis of annual IG returns from all bodies using or holding NHS or social care information
- arbitrate on the interpretation and application of IG policy and give advice
- have oversight of and advise on the confidentiality management and access control frameworks implemented through the National Programme for IT
- own and review the NHS Care Record Guarantee[6] for England annually
- advise the UK Secretary of State on any matters of IG that should be brought to their attention and to produce an annual report to the Secretary of State
- deal with other such matters as required by the Secretary of State and other appropriate bodies
- work with appropriate bodies, across the United Kingdom, on issues within its remit.

[6] The NHS Care Record Guarantee sets out the rules that govern information held in the NHS Care Records Service. The NHS Care Record Guarantee has been drawn up by the Care Record Development Board (CRDB) and is reviewed at least every twelve months as the NHS Care Records Service develops.

2.3.2 The UK Department of Health

The UK Department of Health is committed to improving the quality and convenience of care provided by the NHS and social services. Its work includes setting national standards, shaping the direction of health and social care services and promoting healthier living.

The UK Department of Health has developed a number of codes of practice for the NHS in relation to IG:

- *Confidentiality: NHS Code of Practice* sets out the required standards of practice concerning confidentiality and patients' consent to use their health records
- *Information Security Management: NHS Code of Practice* is a guide to the methods and required standards of practice in the management of information security, for those who work within or under contract to, or in business partnership with NHS organisations in England
- *NHS Information Governance – Guidance on Legal and Professional Obligations* is best practice guidance, which outlines the likely impact of these legal provisions and professional obligations primarily to NHS information but also includes some social care requirements
- *Records Management: NHS Code of Practice* sets out the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.

At a trust (provider) level policies and procedures have been developed based on these codes of practice.

2.3.3 NHS Connecting for Health Information Governance Programme Board

The NHS Connecting for Health[7] (CfH) Information Governance (IG) Programme Board is responsible for the management of overall IG activities within the NHS. The programme board:

- offers advice and guidance on issues referred to it by the NIGB
- ensures that there is appropriate policy, guidance, and advice made available to all NHS Connecting for Health (CfH) teams and providers
- monitors the implementation of IG policy throughout the programme and ensures corrective action is put in place where necessary.

[7] NHS Connecting for Health, an agency of the Department of Health, supports the NHS in providing better, safer care, by delivering computer systems and services that improve how patient information is stored and accessed.

All NHS organisations are required to assess their compliance with IG standards through the IG toolkit. The toolkit is a nationally agreed electronic self-assessment form. It was developed and overseen by the National Health Services Information Authority and is to be continued by the National Programme for Information Technology (NPfIT), which forms part of CfH. Trusts/NHS organisations publish an annual report on compliance with the IG toolkit. The toolkit provides a framework to bring together the requirements, standards and best practice that apply to the handling of information. It has four fundamental aims as follows[14]:

- to support the provision of high quality care by promoting the effective and appropriate use of information
- to encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- to develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- to enable organisations to understand their own performance and manage improvement in a systematic and effective way.

The toolkit is comprised of approximately 100 questions divided into the following topics:

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

The toolkit is constantly evolving to reflect the requirements of and changes in the healthcare environment, with version eight currently in development.

2.3.4 Caldicott Guardian Council UK

The Caldicott Guardian Council UK is an elected body made up of Caldicott Guardians from across the UK. It has developed a strategic work plan setting out its proposals regarding the education, training and development of Caldicott Guardians, communication with the Caldicott community, and developing links with other bodies to highlight decision-makers in the areas covered by IG. The council has the following aims and objectives:

- to be the national body for Caldicott Guardians

- to promote the roles and activities of Caldicott Guardians within the United Kingdom
- to be a forum for the exchange of information, views and experience amongst all Caldicott Guardians
- to seek, consider and to represent the views of Caldicott Guardians on matters of policy relating to the organisation and delivery of IG
- to be a channel of communication upon Caldicott matters with national organisations concerned with the NHS, the independent health sector, local government and health and social care professionals
- to act as a resource centre, provide support and arrange learning opportunities for Caldicott Guardians, both current and of the future.

2.4 Provider governance structures

The Cayton Report [9] recommended that all organisations providing health and social care are required, in addition to having a Caldicott Guardian, to have clear processes within their overall governance structure to ensure compliance, oversight and monitoring of IG within that organisation.

At a provider level the following are in place:

- Caldicott Guardians
- policies and procedures
- the IG toolkit.

2.4.1 Caldicott Guardians

Many of the trusts have appointed a senior manager who has overall responsibility for the IG agenda. At an operational level they also appoint an IG lead and an Information Officer/Caldicott Guardian responsible for IG for that organisation.

The Caldicott Guardian plays a key role in ensuring that the NHS, councils with social services responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information[15]. All organisations are required to have a Caldicott Guardian at a senior level within the organisation.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to facilitate and enable information sharing and advise on options for lawful and ethical processing of information as required. The Caldicott Guardian also has a strategic role, which involves representing and championing IG requirements and issues within the organisation at board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework. This role is particularly

important in relation to the implementation of the National Programme for IT and the development of Electronic Social Care Records and Common Assessment Frameworks. Caldicott Guardians have an important role to play, as part of their broader work on IG, in ensuring that the work of the Registration Authorities[8] is appropriately overseen and that staff are educated about the importance of secure working practices in respect of their smartcards[9]. Ensuring that there is effective governance in place to ensure that the role profiles assigned to staff are appropriate and not overly restrictive or permissive is key to this and it must be remembered that this will be a continuing exercise as staff turnover will inevitably occur(9).

2.4.2 Policies and procedures

A number of the NHS trusts/organisations have developed local IG policies based on the Department of Health Codes of Practice focusing on the four key interlinked strands of openness, legal compliance, information security and information quality assurance. At a provider level IG committees/groups have also been formed to ensure that effective policies and management arrangements covering all aspects of IG are implemented in line with the policy.

2.4.3 The IG toolkit

The origins of the development of the IG toolkit were based on supporting and obtaining assurance that recommendations made in *the Caldicott Review of Patient Confidentiality* in 1997 were being progressed. The original audit method (introduced around 2000/2001) was called the "Caldicott Audit" assessment questionnaire and was completed by trusts and GP practices. This paper audit was replaced with the online IG toolkit in 2002. The toolkit has been reviewed each year with version eight due for release in June 2009. At the time of writing of this report version eight had not yet been released. The annual results are made available to the Care Quality Commission, the National Information Governance Board, Strategic Health Authorities, National Audit Commission and Monitor (for NHS Foundation Trusts) to inform their work.

The toolkit enables organisations to measure annually their compliance with a range of information handling requirements. These requirements include:

---

[8] Organisations that need to access patient information within the NHS Care Records Service and other National Programmes set up Registration Authorities to manage this process. The Registration Authority is responsible for verifying the identity of health care professionals and workers who wish to register to use these services.

[9] NHS CRS Smartcards help control who accesses the NHS CRS and what level of access that they can have. A user's Smartcard is printed with their name, photograph and unique user identity number.

- Data Protection Act 1998, England
- *Confidentiality NHS Code of Practice*
- *International Security Standard: ISO/IEC 27002:2005*
- *Information Security NHS Code of Practice*
- *Records Management NHS Code of Practice*
- Freedom of Information Act 2000, (England).

Table 1 depicts the 2008 result for Aintree University NHS Foundation Trust, indicating the use of the traffic light scoring system[14]. Annual results are published on the CfH website.

Table 1: 2008 IG toolkit result for Aintree University NHS Foundation Trust.

Initiative	Results
Clinical Information Assurance	**83% (GREEN)**
Confidentiality and Data Protection Assurance	**74% (GREEN)**
Corporate Information Assurance	**75% (GREEN)**
IG Management	**82% (GREEN)**
Information Security Assurance	**69% (AMBER)**
Secondary Use Assurance	**84% (GREEN)**

The percentage results indicate the score the Trust has been awarded under each of the six IG topics. The toolkit uses a traffic light scoring system as indicated in the table.

There are different "views" for different types of organisation, for example acute hospital trust, general practice and social care. The first version of the toolkit contained only the acute hospital view. The other versions, in the main, follow the same numbering convention for the criteria but have fewer criteria according to the business of the particular organisation. The contents of a particular view are dependent, in part, on the risk to patient information.

The undertaking of a Privacy Impact Assessment (PIA)[10] for particular projects is an example of one of the requirements of the confidentiality and data protection assurance section of the IG toolkit. In 2007 the Information Commissioner's Office, UK, produced a

[10] A PIA is a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, forsee problems and bring forward solutions.

Privacy Impact Assessment Handbook[16] as a guidance to organisations, to assist them in making their own judgements for each project, which has potential privacy impacts, that they undertake.

The toolkit is also used to assist in protecting the NHS Network. An Information Governance Statement of Compliance (IG SoC) must be agreed between NHS Connecting for Health and all organisations that receive NHS network access, for example general practices. As part of the assurance process for connection, organisations must achieve a minimum standard in selected criteria.

CfH has developed an IG audit, which is a framework for evaluating, assessing and managing the on-going compliance of all entities connected to the NHS network. These audits are conducted by external audit firms and can cover a sample section of the IG toolkit or be more comprehensive. Regular or repeat offenders may find themselves under greater scrutiny.

2.5 Summary

The following significant developments in IG have taken place in England:

- the establishment of the National Information Governance Board (NIGB) in 2005
- codes of practice have been developed by the Department of Health for the NHS in relation to confidentiality, information security management and records management. A report has also been produced on *Information Governance - Guidance on Legal and Professional Obligations*
- each organisation providing health and social care functions has a Caldicott Guardian who is responsible for IG within that organisation
- the IG toolkit which is used as a self-assessment tool for measuring compliance with IG requirements is particularly advanced and facilitates a cycle of ongoing development and improvement for all organisations providing health and social care
- audit of organisations to monitor compliance with IG requirements.

3 Scotland

3.1 Overview

The devolved Government for Scotland is responsible for most of the issues of day-to-day concern to the people of Scotland, including health. Devolution established the Scottish Parliament with full legislative competence across a wide range of devolved subjects. The UK Parliament remains responsible for certain issues, one of which is data protection.

The Scottish approach to health IG has been heavily influenced by the English model. The system is structured at a national level with clear lines of accountability and a self-assessment toolkit, echoing the English IG toolkit, facilitating continuous improvement. Work is ongoing in relation to IG with recent developments in IG standards in 2007 and the subsequent self-assessment tool being relatively new ventures in Scottish healthcare.

In February 2007 NHS Scotland published a *Brief Guide to Information Governance*. The Guide defines IG as a framework for handling information in a confidential and secure manner in accordance with ethical and quality standards. This framework ensures that information is[17]:

- held securely and confidentially
- obtained fairly and lawfully
- recorded accurately and reliably
- used effectively and ethically
- shared appropriately and legally.

NHS IG is one element of the NHS Quality Improvement Scotland (QIS) Clinical Governance and Risk Management Standards. The aim of these standards is to assist NHS boards to develop and improve IG locally. In Scotland, NHS QIS has responsibility for setting national clinical governance and risk management standards and monitoring performance In May 2006, NHS QIS commenced a peer review programme to assess the performance of all NHS Boards against the standards for clinical governance and risk management. In 2007 a report was published detailing national performance against the standards[18]. The audit involved a pre-visit analysis of the self-assessment and evidence provided by NHS boards and the use of a four-point assessment scale reflecting the quality improvement cycle.

The Scottish Executive Health Department views IG as having six main components as follows:

- IG management

- confidentiality and data protection
- freedom of information
- records management
- information security
- information quality assurance.

There have been a number of initiatives aimed at improving systems for handling and managing information. One report of note is that published by the Confidentiality and Security Advisory Group in 2002 – *Protecting Patient Confidentiality*. The report recommended improvements in the way NHS Scotland protects the privacy of patient data while continuing to make data available for the essential purposes of patient care, public health improvement and planning.

3.2 Scottish Legislation

Legislatively the two main areas of focus are the Data Protection Act 1998[11] (UK)[(10)] and the Freedom of Information (Scotland) Act 2002[(19)]. A number of other sources also warrant consideration.

The use of information about patients is governed by[(20)]:

- statute law, e.g. the Data Protection Act 1998[(10)], the Human Rights Act 1998[(21)], the Infectious Disease (Notification) Act 1889[(22)] and the Freedom of Information (Scotland) Act 2002[(19)]
- the common law in Scotland on privacy and confidentiality (which requires either consent or a legal or public interest for disclosure)
- professional standards
- the policies and organisational standards of the Scottish Executive Health Department (SEHD) and NHSScotland, underpinned by the Confidentiality and Security Advisory Group for Scotland (CSAGS) report, 2002[(23)].

3.2.1 The Data Protection Act 1998 (UK)

The Data Protection Act 1998 came into force in March 2000. Its purpose is to protect the right of the individual to privacy with respect to the processing of personal data. It provides a framework that governs the processing of information which identifies living individuals. Processing includes obtaining, recording, holding, using and disclosing information. The legislation applies to all forms of records including paper, electronic and other images. It requires organisations to process fairly and lawfully any information which might enable a patient to be identified.

[11] This is the same Data Protection Act that governs data protection in England. There are differences however between the Freedom of Information Acts.

A key requirement is schedule 1 of the Data Protection Act, which requires organisations to process fairly and lawfully any information which might enable a patient to be identified. Organisations must comply with the *Fair Processing Code*. Amongst other things, this code requires patients to be informed of the identity of the data controller. The term data controller is used in the 1998 legislation to describe organisations that process personal data. In the case of NHSScotland, data controllers are the organisations that collect information from patients. It might be a general practice, NHS trust, an NHS board or a special health board. Responsibility for complying with the provisions of the Data Protection Act rests with each organisation as a whole, with chief executives bearing the ultimate responsibility for the actions of their staff.

In order to be lawful, the Information Commissioner takes the view that data controllers must comply with both statute and with the common law. This has a bearing on the need for patients to give consent before patient identifying information is shared. The common law in Scotland is based on precedent. As a result its impact is not always clear and it may change over time. Whilst various interpretations of the common law may be possible, there is widespread acceptance that it reinforces the need to obtain consent from patients before sharing their information[(23)]. Implied consent is acceptable in circumstances such as GP referral. Consent is not required in instances where the data has been anonymised but patients do have a right to know when it is intended that their information will be anonymised for a range of appropriate purposes.

The Data Protection Act requires organisations to use the minimum amount of information on a need to know basis and to retain it only for as long as is needed for the purpose for which it was originally collected[(20)].

3.2.2 The Freedom of Information (Scotland) Act 2002

The Freedom of Information (Scotland) Act 2002[(19)] provides a right of access to information held by Scottish public authorities, creates exemptions from the duty to disclose information and establishes the arrangements for enforcement and appeal. The FOI Act came into force on 1 January 2005 and ensures that any person requesting information from a public body will receive that information, subject to certain exemptions. It encourages public authorities to be more open and accountable, and to organise their information in an efficient and accessible way. The provisions of the FOI (Scotland) Act are enforced by the Scottish Information Commissioner, a fully independent public official. It is noteworthy that the Scottish Information Commissioner is completely independent of the UK Commissioner. The Scottish Information Commissioner's duties include:

- the promotion of good practice
- approving and assisting in the preparation of publication schemes

- providing information on the operation of the act
- enforcing compliance with the act.

It is worthy of note that the Scottish Information Commissioner does not have responsibility for enforcing data protection legislation – it is the responsibility of the UK Information Commissioner.

3.3 National structures for information governance

The following are the structures in place in Scotland to oversee IG:

- The Confidentiality and Security Advisory Group for Scotland (CSAGS)
- The Information Services Division (ISD) of NHS National Services Scotland (NSS)
- The Caldicott Framework
- professional standards
- NHSScotland codes of practice.

3.3.1 The Confidentiality and Security Advisory Group for Scotland

The Confidentiality and Security Advisory Group for Scotland (CSAGS) was established in September 2000 as an independent committee, supported by the Scottish Executive Health Department (SEHD), to provide advice on the confidentiality and security of health related information to the Scottish Executive, the public and healthcare professionals. The group consists of 20 members from a variety of professions and interest groups. The role of the CSAGS is:

- to set national standards to govern the confidentiality and security of patient information within the NHS and with outside voluntary and private agencies
- to provide guidance on patient rights and NHS requirements for information
- to provide guidance and support to Caldicott Guardians
- to develop a new code of practice on the confidentiality of personal health Information for the NHSScotland and a national protocol for sharing information between health, housing, social work etc.
- to advise on the confidentiality and security aspects of implementing the *Information Management and Technology Strategy*
- to input to policy making, for example the development of electronic patient records.

CSAGS recommended that data flows should be anonymised whenever possible and that there should be a central service to anonymised national data. In response to this, ISD

undertook a fundamental review of its processing of the national data sets. The results of this review and a set of good practice guidelines are set out in the following reports:

- *Managing Patient Identifying Data: Best Practice Guidelines* [24]
- *Anonymisation: NHSScotland National Data Sets* [25]

3.3.2 Information Services Division of NHS National Services Scotland

NHS National Services Scotland is a non-departmental public body accountable to the Scottish Government. NSS provides national strategic support services to and advice to NHSScotland[12]. The role of NSS includes caring for patients directly, promoting long-term health improvement, delivering efficiency and cost-effectiveness to NHSScotland and providing information to clinicians, the public and the Scottish Government. Services are delivered through a number of divisions. In relation to IG the Information Services Division (ISD) is of most relevance.

The ISD is Scotland's national organisation for health information and statistics. ISD has developed, and continues to develop, systems that underpin the collection, management, analyses and presentation of information. It works in partnership with health boards, hospitals, GPs, local authorities, voluntary organisations and others to analyse data to inform research, support decision-making and stimulate debate, all with the ultimate aim of improving Scotland's healthcare.

The Scottish Executive Health Department (SEHD) tasked the NHS National Services Scotland (NSS) with establishing an IG programme for NHSScotland. The ISD has set up a formal programme of work to do this and has a small team in place to develop, implement and progress the programme.

The IG team, based in ISD, supports NHSScotland staff by:

- offering an in-depth knowledge of the individual elements of IG
- developing and publishing IG standards
- developing tools to support compliance with the standards
- facilitates national forums such as the NHSScotland Data Protection Forum and the IT Security Officers Forum.

The IG team works closely with NHS Education for Scotland (NES), NHS Quality Improvement Scotland (QIS) and various forums that represent groups within NHSScotland. These partnerships have helped to develop a range of standards, tools and educational initiatives to support NHSScotland to meet its IG commitments.

[12] NHS Scotland comprises 14 territorial NHS Boards responsible for the planning and delivery of all health services in their own area

In September 2007 NHSScotland set out IG Standards as agreed with the Scottish Executive Health Department and NHS Quality Improvement Scotland[13] (NHS QIS). A review of the NHS IG in England carried out at the end of 2005 called for a strengthening of existing requirements for organisations to have IG steering groups or boards as outlined in the IG toolkit. A similar review in Scotland has led to the development of IG standards and a self-assessment toolkit for NHSScotland. The IG toolkit for NHSScotland assists organisations in complying with the IG initiative, and record progress against IG standards in the following areas:

- IT security
- Caldicott Guardians
- data protection
- freedom of information
- records management (including management of corporate and clinical records)
- quality management.

The toolkit is a web-based tool, enabling the NHS boards to record progress against the IG standards contained within the toolkit.

3.3.3 The Caldicott Framework

In March 1999 a Caldicott Framework was set up to respond to the recommendations of the Caldicott Committee in its *Report on the Review of Patient-Identifiable Information*. The report made a number of recommendations for regulating the use and transfer of person identifiable information. Central to the recommendations was the appointment in each NHS organisation of a "guardian" of person-based clinical information to oversee the arrangements for the use and sharing of clinical information. The framework requires each NHSScotland organisation to appoint a senior clinician such as the medical director as Caldicott Guardian(26).

The UK Council of Caldicott Guardians is an elected body made up of Caldicott Guardians from health and social care across the UK. There are three elected members from NHSScotland. The aims and objectives for the Council are as outlined in section 2.3.4(26).

In 2007 the Scottish Executive published a *Caldicott Guardian Manual*(26) detailing the role of the Caldicott Guardian. The manual makes reference to organisation type and associated requirements. Individual general medical and dental practices, pharmacists

[13] NHS Quality Improvement Scotland is responsible for publishing standards for information governance which are used to assess NHS boards' effectiveness in this area of activity. NHS QIS conducts an annual assessment requiring NHS boards to complete a self-assessment which is verified by a subsequent visiting and verification process.

and opticians do not need to appoint a Caldicott Guardian, but do need to have an IG lead who, if they are not a clinician will need support from a clinically qualified individual. It is the responsibility of NHS boards and community health partnerships to ensure that, within every practice there is an IG lead who provides support and guidance as required.

3.3.4 Professional standards

All healthcare professionals must maintain standards of confidentiality laid down by their professional body, such as the Scottish General Medical Council. As a rule, such standards have been developed to clarify what the law means in a healthcare setting and to set out any additional principles or ethical standards for that profession.

3.3.5 NHSScotland Codes of Practice

NHSScotland has developed the following codes of practice relating to IG:

The NHS Scotland Code of Practice on Protecting Patient Confidentiality

The *NHS Scotland Code of Practice on Protecting Patient Confidentiality* [20] was published in 2003 by the Scottish Executive Health Department. It provides guidance to NHS employees on the necessary safeguards to maintain patient confidentiality. NHSScotland staff are contractually obliged to adhere to the code [20].

The NHS Scotland Information Security Policy

An *NHS Scotland Information Security Policy Statement* [27] was published in 2006 by the Scottish Executive Health Department Directorate of Primary Care and Community Care. This policy statement updated the *NHSScotland IT Security Policy* which had been established in 1993. The aim of the policy is to safeguard the confidentiality, integrity and availability of all forms of information within NHSScotland. Its purpose is to protect personal and corporate information from all threats, whether internal or external, deliberate or accidental. A comprehensive framework is in place to support the policy. This takes the form of a series of policy, standards and best practice guideline documents on all aspects of IT security in NHSScotland organisations.

Records Management: NHS Code of Practice

In July of 2008 the Scottish government published a code of practice for records management [28]. This details best practice in relation to the creation, use, storage, management and disposal of NHSScotland records.

3.4 Provider structures for information governance

A number of initiatives have been undertaken at a provider level to improve IG initiatives. These are based on legislation, the common law, and a series of pre-existing professional and organisational standards. The provider structures in place, similar to those in England, are as follows:

- Caldicott Guardians
- policies and procedures
- the IG toolkit
- *The Competency Framework for Information Governance*.

3.4.1 Caldicott Guardians

Similar to the English model, each NHS organisation is required to appoint a Caldicott Guardian.

The key Caldicott responsibilities relate to:

- strategy and governance
- confidentiality and data protection expertise
- internal information processing
- information sharing.

3.4.2 Policies and procedures

A number of NHS organisations have developed more localised policies and procedures to implement IG initiatives. These are based on the high level NHS codes of practice that have been developed at a national level.

3.4.3 The IG toolkit

The electronic IG toolkit was launched in Scotland in March 2007 to assist NHS organisations in complying with the national IG initiative and record progress against IG standards in a number of areas. The use of the toolkit fosters a culture of continuous development and improvement in relation to IG at a provider level. It is based on the English toolkit but has been adapted to suit the Scottish system. The Scottish toolkit categorises IG in the following areas:

- IT security
- Caldicott Guardians

- data protection
- freedom of information
- records management (including management of corporate and clinical records)
- quality management

3.4.4 The Competency Framework for Information Governance

The importance of education and training around IG issues for staff has been identified and is an area very much to the fore of the IG agenda. In 2008 NHS National Services Scotland and NHS Education for Scotland collaborated to develop a *Competency Framework for Information Governance*[29]. This framework was developed in response to the challenges and risks faced by NHS boards and acts as a key tool to assist with the planning and implementation of local workforce development initiatives.

3.5 Summary

The following significant developments in IG have taken place in Scotland:

- all NHS organisations are accountable for their performance against national standards for health IG
- a self assessment tool has been developed based on the English IG toolkit
- each organisation providing health and social care functions has a Caldicott Guardian who is responsible for IG within that organisation
- In 2008 NHS National Services Scotland and NHS Education for Scotland collaborated to develop a *Competency Framework for Information Governance* [29]
- NHS Scotland has published codes of practice on records management and on protecting patient confidentiality. An NHSScotland information security policy has also been published.
- NHS Quality Improvement Scotland audit of compliance with IG requirements, conducted as part of an overall audit of clinical governance and risk management standards.

4 Canada

4.1 Overview

Canada is a federal state consisting of ten provinces and three territories. The federal government is responsible for matters that concern Canada as a whole, such as international trade and national defence. The provinces have independent constitutional powers in areas such as education, taxation and healthcare. The territories do not have exclusive legislative powers. Federal laws regulate the election of territorial councils, whose powers – including passing territorial laws – are conferred by the federal government.

There is considerable variety in the types, sizes and complexity of IG structures within which healthcare providers and healthcare organisations operate in Canada. There are a number of pan-Canadian IG mechanisms in place however most of the structures and systems in place provincially are at different levels and are by no means nationally cohesive. This is primarily due to legislative differences between the provinces.

Many healthcare organisations, recognising the importance of IG, have established structures and processes with a chain of accountability for handling privacy breaches and security incidents. For example, a healthcare institution's board of directors may be established by legislation that outlines the general rules for the existence and operation of a specific healthcare organisation or facility. The privacy and security obligations for that organisation or facility are typically contained in separate privacy legislation which applies to the collection, use and disclosure of personal health information in the jurisdiction within which the organisation or facility operates, for example Ontario's Personal Health Information Protection Act, 2004[30].

4.2 Legislation

Although there is no pan-Canadian legislation relating to IG there is commonality across the provinces. The protection of personal health information is regulated by various privacy laws across Canada which, in turn, establish standards both for health IG and for patient privacy rights. For example most provinces and territories have enacted freedom of information and protection of privacy statutes to protect personal information in the custody or control of public or government bodies, including publicly funded healthcare sector entities, such as hospitals, and in such jurisdictions where they exist, regional health authorities or health agencies.

Similarly, the federally regulated public sector has privacy legislation in place to cover both personal information and personal health information in the custody and control of federal government bodies (i.e. the Privacy Act)[31]. There also exists federal private

sector legislation, namely the Personal Information Protection and Electronic Documents Act (PIPEDA)[32] that applies to both federal and provincial entities in the course of conducting commercial activities[33].

Health IG is informed by a combination of legal, ethical and regulatory requirements for the collection, use or disclosure of personal health information. The current framework that applies to healthcare providers in Canada is made up of the following:

- privacy laws and regulations in effect in different Canadian jurisdictions
- health-related legislation with specific confidentiality provisions or with restrictions on the collection, use or disclosure of personal health information (i.e. provincial public hospital acts or medical care insurance acts that either prohibit third-party disclosures or contain specific confidentiality provisions)
- *The Canadian Standards Association's Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96)[34]
- professional codes of ethics and health privacy codes or guidelines created by health professional associations and professional standards of practice and professional misconduct regulations set by the health regulatory colleges
- common law medical confidentiality obligations and administrative rulings issued by professional regulatory colleges and by Information and Privacy Commissioners.

While Canadian privacy laws are lengthy and complex, most are based on internationally accepted fair information principles which form the basis for the ten privacy principles set out in *Canadian Standards Association's Model Code for the Protection of Personal Information*. These principles are widely regarded as an important governance model[35]. They are:

- accountability for personal information
- identifying purposes for the collection of personal information
- obtaining consent
- limiting the collection of personal information
- limiting the use, disclosure, and retention of personal information
- ensuring the accuracy of personal information
- ensuring safeguards for personal information
- granting individuals access to their personal information
- openness and transparency about personal information practices
- challenging compliance.

4.3 National structures for information governance

Provincially varying laws shape the way IG is structured and there is considerable variety in the types, size and complexity of IG structures within which healthcare

providers and organisations operate in Canada. However, efforts are being made to move towards a more inclusive, pan-Canadian approach.

Healthcare providers can rely on a variety of established mechanisms to assist them in compliance with legislative privacy and security rules and requirements, for example privacy and security teams. There are also further tools available such as the *ACIET Pan-Canadian Health Information Privacy and Confidentiality Framework* and the *College of Physicians of Alberta: Medical Informatics Committee's Data Stewardship Framework*[36]. These provide guidance on common and consistent statutory provisions in addition to IG requirements and mechanisms.

In an attempt to harmonise existing Canadian privacy regimes, the Federal/Provincial/Territorial Conference of Deputy Ministers of Health tasked its Advisory Committee on Information and Emerging Technologies (ACIET)[14] with developing a *Pan-Canadian Health Information Privacy and Confidentiality Framework* ("the ACIET Framework")[37]. 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 and private healthcare sectors and serves as a tool for regulators as they seek to develop consistent privacy requirements through the introduction or amendment of health privacy legislation. The *ACIET Framework* was finalised in January 2005 and endorsed by the Federal/Provincial/Territorial Conference of Deputy Ministers of Health, with the exception of Saskatchewan and Quebec. The *ACIET Framework* continues to serve to inform and influence the development and review of health privacy statutes in Canada[33].

There are a number of existing initiatives to be found among Canada's provinces and territories which can be adapted to fit local needs and statutory requirements. Policies and procedures have been developed at a provider level based on these. The interlinked websites of the various Information and Privacy Commissioners, as established through legislative provisions, across the country provide guidance in relation to this. Most privacy policies are based on the principled approach used in the *Canadian Standards Association (CSA) Model Code*[34], which has been formally incorporated as schedule one of the Personal Information Protection and Electronic Documents Act (PIPEDA).

The *ISO 17799 Security Standard – Information Technology – Code of Practice for Information Security Management*[38] – has been adopted for use by the British

---

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

Columbia Health Information Standards Council. The Ontario Health Information Standards Council has also endorsed a portion of this standard that recommends the use of written security policies.

As can be seen in the information detailed above, Canada is lacking a nationally cohesive and structured approach to IG; there is however commonality among a number of the provinces. This fragmentation is mainly owing to the differing legislative provisions across the territories and provinces. However, efforts are being made to rectify this and to develop pan-Canadian mechanisms to support IG. This emerged in a White Paper developed by Canada Health Infoway in 2007 discussing *Information Governance of the Interoperable Electronic Health Record (EHR)*[33]. The governance issues arising from this will naturally affect the health sector nationally and will need to be dealt with accordingly.

4.4 Provider structures for information governance

At a provider level much has been achieved in respect of the governance of health information within the different healthcare settings. The sections that follow detail examples of IG structures and practices that that are in place at the different levels of care. At each level of care a specific case study has been documented.

4.4.1 Privacy Officers

In the Canadian healthcare system, healthcare providers are ultimately responsible for the personal information in their custody or control. The role of the Privacy Officer is similar to that of the Caldicott Guardian in the UK. The tasks involved in ensuring privacy protection can however be delegated to a staff person designated as the Privacy Officer who then carries out these tasks to promote compliance, particularly in large healthcare organisations. The most important roles of a Privacy Officer are as follows[39]:

- to understand the requirements of applicable legislation
- to provide ongoing privacy and security training
- to answer questions about data protection and security from staff, patients and the public about the various data protection policies of the healthcare institution or practice.

Privacy Officers play a key role in investigating suspected problems and managing problems as they arise. They should also form part of the business team responsible for policy, process and technology decisions to ensure that privacy and confidentiality are considered and privacy enhancing solutions are adopted where possible.

In many organisations, the role of the Information Security Officer is also essential to achieving robust data protection and security practices. Information Security Officers are responsible for information security management and technology. They work closely with Privacy Officers and are typically assisted by teams that, in large healthcare organisations, cross organisational boundaries.

4.4.2 Primary care practices

In Alberta the Physician Office System Program (POSP) which was created in 2001, has developed a programme policy related to IG and supports providers responding to IG issues in the primary care setting. POSP operates under a tri-partite governance agreement between Alberta Health and Wellness, the Alberta Medical Association and Alberta's nine Regional Health Authorities (RHAs). These three organisations appoint representatives to the POSP Committee, who in turn make operational decisions related to the programme. POSP is supported by a programme management office. Other provinces are embarking on similar physician automation initiatives, which serve the same purpose as POSP in that they subsidise physicians' implementation of pre-qualified or certified EMR systems. However, the POSP program is currently the most broadly adopted program, with more than 61 % of Alberta physicians enrolled in the program as of June 2006[33].

4.4.3 Hospital settings

University Health Network (UHN) in Toronto comprises three sites and provides services to approximately 30,000 inpatient cases. Ultimate accountability for UHN's compliance with the Personal Health Information Protection Act (PHIPA)[30] rests with the Board of Governors and the hospital's President and Chief Executive Officer. The IG practices are overseen by the UHN Privacy Officer under the direction of the Privacy Manager who reports to the hospital's Executive Vice-President and Chief Information Officer. They in turn report major privacy breaches and security incidents to the President and CEO and to the hospital's Board of Governors[33].

4.4.4 Regional health authorities

The Vancouver Coastal Health (VCH) Authority is responsible for providing five different health services across 550 sites in British Columbia. VCH draws primarily on the Freedom of Information and Protection of Privacy Act[40] for its IG processes. It is also subject to British Columbia's Regional Health Authorities Act[41] which sets out the conditions under which regional health boards are designated and the RHAs are incorporated and created, as well as the duties and responsibilities of these boards. In May 2006 VCH created an Information Governance Steering Committee and a working

group with respect to health information privacy and governance. The steering group includes the Chief Executive Officer, Chief Information Officer, Vice-President of Employee Engagement, and Vice-President of Medical Clinical Quality and Safety, Legal Council and Director of Client Relations and Risk Management. The committee meets on an as-needed basis to discuss privacy and information security risk management issues and compliance measures, among other governance issues. The working group, comprised of 25 members, was created in tandem with the steering committee to help vet policies, change management processes and assist with the shift to an electronic health record environment. The privacy and IG structures at VCH are based on a centralised model with uniform applications across all healthcare providers and all affected organisations across the region. VCH is governed by one common *Regional Information Privacy and Confidentiality Policy* with respect to its personal information privacy practices and has created one centralised Information Privacy Office for the entire region. This office is currently supported by one regional manager and two privacy officers, supplemented periodically by contract project resources. The investigation and containment of a privacy breach at any facility within the region is coordinated centrally through the Information Privacy Office(33).

4.4.5 Government funded health agencies

Many health care organisations throughout Canada have established privacy and security teams as a means of detecting data protection problems and assisting with compliance with applicable laws and institutional policies and procedures.

Cancer Care Ontario (CCO) is a provincially funded planning and research organisation that advises the Ontario government on all aspects of provincial cancer care. The organisation has appointed a Chief Privacy Officer (CPO) who reports directly to the President and CEO and oversees the organisation's privacy compliance program. It has also established a core privacy team that includes privacy leads who are responsible for ensuring privacy policies are adhered to and data stewards who ensure data holdings are managed in accordance with their identified purposes. The organisation also has a security team which includes the Chief Information Officer, Director of Information Technology and a Systems Security Specialist. Key components of the privacy compliance program include privacy policies and related procedures, mandatory employee privacy and security orientation, training programmes and privacy impact assessments on CCO data holdings and new proposals(33).

4.4.6 Provincial health information infostructure[15]

Alberta and Newfoundland and Labrador are among the provinces that have a coordinated, province-wide health information infostructure.

[15] Infostructure refers to the IT infrastructure or information infrastructure of an organisation.

The Newfoundland and Labrador Centre for Health Information (CHI) was established to provide quality information to health professionals, the public and health system decision makers. Through collaboration with the health system, the CHI supports the development of standards, maintains key provincial health databases and prepares and distributes health reports. The centre's mandate also includes the development of a confidential and secure health information network to serve as the foundation for the provincial EHR. The centre is divided into four divisions as follows:

- health information network
- data quality and standards
- research and evaluation
- privacy and corporate services.

Alberta's approach to IG at the provincial level is via a Data Stewardship Committee. Alberta established the Electronic Health Record Data Stewardship Committee in 2003 by ministerial order. Membership is limited to 12. The legislative environment in Alberta is such that Alberta Health and Wellness (AHW) acts as an information manager of healthcare providers participating in the EHR. As an information manager the AHW provides the infostructure for the operation of the provincial EHR and enters into agreement regarding its development on behalf of all participating custodians. This information management relationship between AHW and the information custodians is laid out in a master Data Sharing Agreement that binds participants to an Information Exchange Protocol (IEP), which in turn describes the purposes for which personal health information in the EHR must be used. It also expressly limits secondary uses of data (research cannot be conducted using data from the EHR). The Data Sharing Agreement and IEP are the primary vehicles through which the Alberta EHR is governed[33].

4.5 Summary

The following significant developments in IG have taken place in Canada:

- efforts have been made toward a more pan-Canadian approach in the development of the *Canadian Standards Association Model Code*, the *ACIET Framework* and the PIPEDA, providing guidance to healthcare providers
- Privacy Officers are in place in healthcare organisations, carrying out a similar function to the Caldicott Guardians in the UK
- although not nationally cohesive, policies, procedures and standards for health information are in place across all healthcare settings.

It has been recognised that a national approach is more desirable and efforts are being made to achieve this. As can be seen from the information detailed above a number of

areas of good practice have been identified at a provincial level that could be applied nationally.

5 Australia

5.1 Overview

Australia operates a federal system of government in which power is divided between the Commonwealth Government and the six state governments. The Commonwealth Government is responsible for passing legislation relating to issues that concern Australia as a whole such as taxation, defence and foreign affairs. The states retain legislative power over all other matters that occur within their borders, including education and health. Each state has its own constitution. Three of the ten territories have been granted a limited right to self-government by the Commonwealth and a range of issues are now handled by a locally-elected parliament. The other seven territories continue to be governed by Commonwealth law.

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). The latest version of this agreement came into effect in September 2004. The structures and systems have borne witness to many shifts and changes in arrangements and priorities over the years but the overall basic structure is still recognisable despite the changes incorporated to cope with an ever-changing health landscape. Of central importance to IG is the National e-Health and Information Principal Committee (NEHIPC) and its standing committees as follows:

- National Health Information Standards and Statistics Committee (NHISSC)
- Population Health Information Development Group (PHIDG)
- National Advisory Group on Aboriginal and Torres Strait Islander Health Information and Data (NAGATSIHID)
- National Health Performance Committee.

The agreement demonstrated that, with support, it has the potential to provide much of the governance structure needed to provide good quality, national health data. This includes the NEHIPC and a host of other stakeholders[42].

EHealth is a focus point in Australia with the development of a Unique Health Identifier[16] (UHI) high on the agenda. The National Electronic Health Transition Authority (NEHTA) is developing the requirements for a unique, nationally applicable individual healthcare identifier (IHI). The implementation of this will have obvious implications for IG – primarily around privacy and security of information. Mindful of this NEHTA has published *Privacy Blueprint – Unique Health Identifiers*[43], which sets out a

[16] A UHI is defined as the designation permanently assigned to an individual for identification and should be governed by an independent central trusted authority[2].

systematic framework to consider the privacy issues raised by the collection and use of information involved with the UHI service.

5.2 Legislation

As in Canada, there is no specific health information act at a national level. In the absence of this certain states and territories have enacted specific health information legislation[44].

5.2.1 Federal legislation

The relevant federal legislation is the Privacy Act 1988[45] and the Privacy (Amendment) (Private Sector) Act 2000. The 2000 Act applied the ten national privacy principles in the 1988 Act to health service providers in the private sector[44]. The ten national privacy principles cover:

- collection
- use and disclosure
- data quality
- data security
- openness
- access and correction
- identifiers
- anonymity
- transborder data flows
- sensitive information.

5.2.2 State legislation

A number of states and territories have enacted specific health information legislation, for example New South Wales: Health Records and Information Privacy Act 2002[46].

The Health Records and Information Privacy Act 2002 (HRIP Act)[46] came into effect on 1 September 2004. It governs the handling of health information in the public sector, and it also seeks to regulate the handling of health information in the private sector in New South Wales (NSW). In December 2004 Privacy NSW developed four statutory guidelines under the HRIP Act. These guidelines are legally binding documents that define the scope of particular exemptions in the health privacy principles in the following areas:

- use or disclosure of health information for the management of health services

- use or disclosure of health information for training purposes
- use or disclosure of health information for research purposes
- notification when collecting health information about a person from someone else.

5.3 National structures for information governance

The Australian health system has quite a structured model in place with regard to areas of responsibility in health information. The following structures are in place in relation to IG:

- National eHealth and Information Principal Committee
- National Health Information Standards and Statistics Committee

Figure 1, taken from the Australian Institute of Health and Welfare website, explains the overall structure and reporting systems[47].

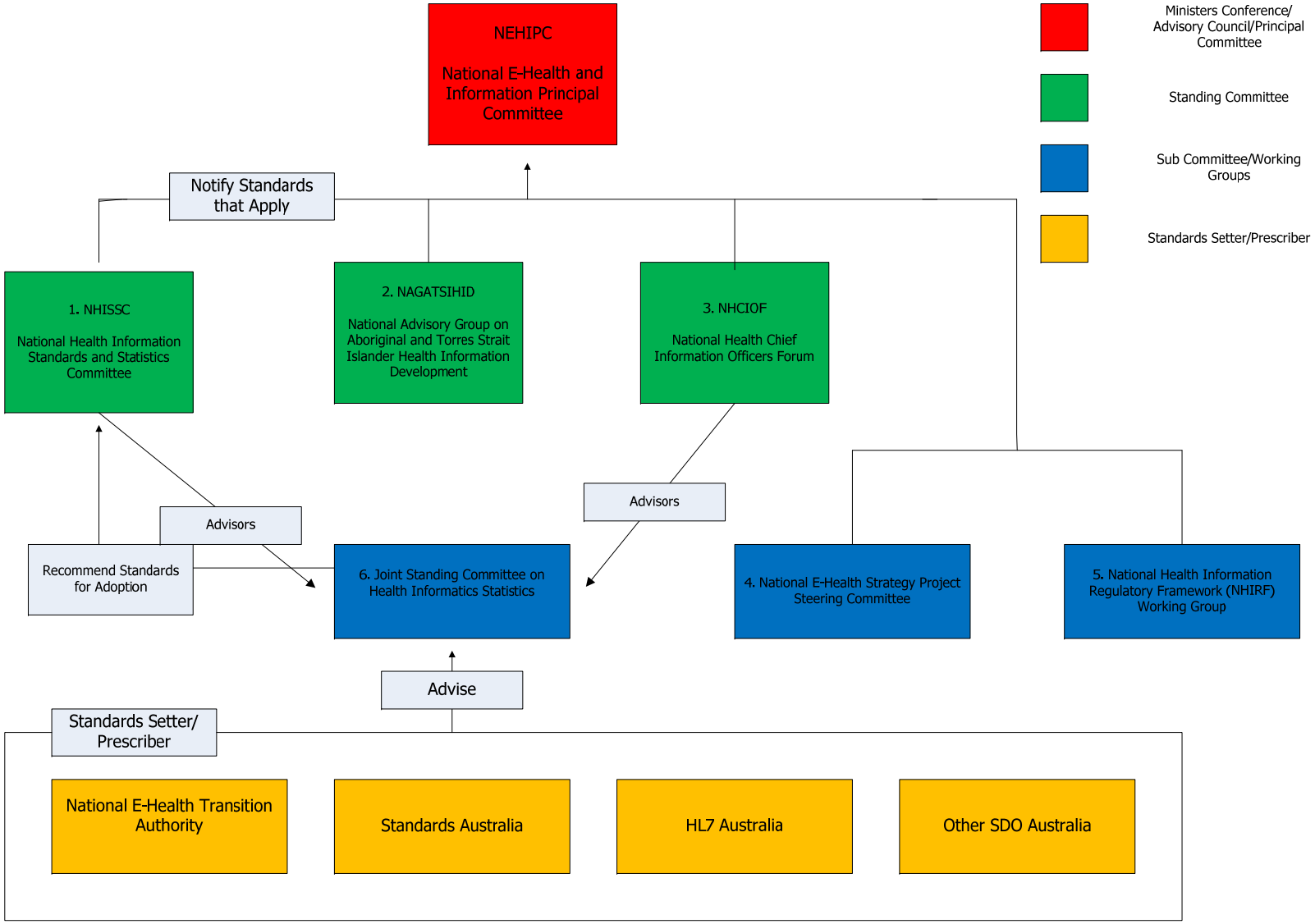


Figure 1, Australian Health Information Structure (From the Australian Institute of Health and Welfare website).

5.3.1 National eHealth and Information Principal Committee

The Principal Committee reporting to the Australian Health Ministers Advisory Council (AHMAC) on information plays a key role in ensuring there is central coordination across all governments and related agencies in relation to nationally relevant health information. The Principal Committee oversees subcommittees which negotiate and determine data standards and national initiatives to drive good quality data. In January 2008, AHMAC agreed to reconstitute its principal information committee to include eHealth alongside its existing focus on information management. Reflecting this broader focus, the principal committee has been renamed the National eHealth and Information Principal Committee (NEHIPC). As the eHealth agenda plays out in Australia, the current methods of collecting information for the purposes of management, policy and research will be challenged. Work is well underway to examine the potential for harnessing information from new sources as well as the potential impacts on current data pathways. The need to balance the public health use of information with community concern about personal privacy presents a key challenge for the health information system and therefore a strong IG framework will facilitate an appropriate balance being struck[48]. The NEHIPC is pivotal to achieving this goal.

The role of the NEHIPC is to advise AHMAC on eHealth and information strategies and to facilitate collaboration between the Commonwealth, states and territories to implement eHealth and information strategies. Responsibilities and key tasks in relation to IG for NEHIPC include:

- develop a national eHealth Strategy to improve health outcomes through national collaboration in agreed priority areas for action over the next five years
- develop a national information management and technology implementation plan that reviews the scope, funding, governance and timetabling of existing information management and technology projects, in consultation with AHIC
- advise on national policy and legislative frameworks to support the national implementation plan
- promote alignment and collaboration at a local level
- oversee the development and publication of health performance reports
- endorse national information standards
- oversee the implementation and ongoing development of a National Health Information Agreement.

The NEHIPC outline four key priorities to support the overall national health agenda in their strategic work plan for the period 2007/08 to 2012/13. The first of these is a stronger national approach. The work plan states that strategic planning and coordination at the national level will help to ensure a high degree of consistency and alignment so as to reduce duplication, wasted effort and expense.

The three further priorities that have been identified are:

- better use of health information to improve the quality of the health system: utilising health information to improve clinical care and reduce errors
- better health information for consumers: enhancing the ability of consumers to make informed decisions about their health and wellbeing. Consumers also need to be assured that their personal healthcare information is protected by appropriate data protection arrangements.
- better outcomes from targeted investment in health information: enhancing the scope and coverage of health information through research, building on existing data collections, data linkage and better health outcomes monitoring. This includes improving the quality and utility of information currently collected and addressing any emerging gaps and information needs.

5.3.2 The National Health Information Standards and Statistics Committee

The NEHIPC work program is supported by a number of standing committees and time-limited working groups that are established for specific purposes. The Standing Committees under the auspices of the NEHIPC assume responsibility for various programmes and report to the NEHIPC. In relation to IG the National Health Information Standards and Statistics Committee (NHISSC) is of most relevance.

As outlined in figure 1, Standards Australia[17] is one of the bodies that provide advice to the Joint Standing Committee on Health Information Statistics and in turn the NHISSC. Standards Australia has been involved in developing standards for information security management. In 2005 Standards Australia launched a new governance standard for information and communication technology. AS 8015 is the first in a series of standards and companion publications developed to provide guidelines for directors on the effective, efficient and acceptable use of information and communication technology within their organisation.

5.3.3 Privacy Regulation

Similar to the Canadian model, the Australian system can be described as somewhat fragmented in that legislation and provisions differ across the states and territories. Provisions in relation to privacy are described below.

Public sector regulation of privacy in Australia is of three types(49):

[17] Standards Australia is a non-government standards organisation charged by the commonwealth government to meet Australia's need for contemporary, internationally aligned standards and related services.

- confidentiality or secrecy provisions. All nine jurisdictions have such regulation that can apply generally (e.g. to all employees and all information) or specifically (e.g. to some employees and to specific types or registers of information)
- privacy legislation or regulation applying to all public agencies. The Commonwealth, the Australian Capital Territory, New South Wales, the Northern Territory and Victoria have legislation of this type. All other jurisdictions, except Western Australia, have relied on administrative guidelines. These would generally be treated as subject to other legislation, a status that is made explicit in Queensland
- health information privacy legislation that limits handling of health information. New South Wales and Victoria have such specific legislation, while the Northern Territory includes such information specific controls in the general legislation.

Efforts are being made however to adopt a more pan-Australian approach. At the time of writing, the Department of Health and Ageing (Australia) is developing a national health privacy code. The code is an initiative of the Australian Health Minister's Advisory Council. The objective of the code is to achieve consistency across the public and private sectors through a single national code for the appropriate collection and handling of information.

All organisations that provide a health service are covered by the Privacy Act 1988. The Office of the Privacy Commissioner has published *Guidelines on Privacy for the Private Health Sector*[50] in addition to a number of information sheets relevant to health IG including[18]:

- sharing health information to provide a health service
- disclosure of health information and impaired capacity
- use and disclosure of health information for management, funding and monitoring of a health service
- taking reasonable steps to make individuals aware that personal information about them is being collected
- information privacy principles under the Privacy Act 1988.

The above mentioned information sheets, and others besides, cover a number of IG topics and provide guidance to healthcare providers in both the public and private sectors.

5.4 Provider structures for information governance

Few initiatives can be identified at a provider level in Australia. Efforts are being made towards a more structured national approach which should then inform developments at

[18] Available on the website of the Office of the Privacy Commissioner: http://www.privacy.gov.au/materials/types/infosheets?sortby=32

a provider level. Guidance is available for providers in the form of Health Records and Information Privacy Act and the guidelines published by the Office of the Information Commissioner, as outlined above. Provider level policies and procedures could be developed based on these.

5.5 Summary

The following significant developments in IG have taken place in Australia:

- the development of the NEHIPC reflects the broader focus of health information as the e-health agenda develops
- all healthcare providers, both public and private are governed by the provisions of the Privacy Act 1988
- the Office of the Privacy Commissioner has published guidelines and additional information sheets in relation to IG requirements.

The strategic work plan of the NEHIPC is to cover the period 2007/08 to 2012/13. As such it is likely that the framework could be better assessed over time and following the achievement of the goals as set out in the work plan. However, the Australian approach to date has been quite structured with an emphasis on the development of an integrated and cohesive framework – similar to the English and Canadian experiences.

6 New Zealand

6.1 Overview

New Zealand is a constitutional monarchy with a parliamentary democracy. It has no separately represented subnational entities such as provinces or states, apart from local government. The only body which can pass legislation is the elected House of Representatives.

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 structures. The *WAVE Report - From Strategy to Reality*[51] 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*[52] was launched resulting in the restructuring of a number of health information committees. Transformation is continuing with reforms ongoing in 2008 and 2009.

6.2 Legislation

Legislatively, it is the Privacy Act 1993[53] which is of primary importance in New Zealand. This led to the development of a Health Information Privacy Code[54] in 1994, which is one of the cornerstones of health IG in New Zealand.

6.2.1 The Privacy Act 1993, New Zealand

The Privacy Act 1993[53] sets out 12 information privacy principles on collecting, using, keeping, disclosing, transferring, accessing and securing personal information[44].

Principles one to four govern the collection of personal information. These include the reasons why personal information may be collected, where it may be collected from, and how it is collected. The general rule is that it should be collected from the individual concerned.

Principle five governs the way personal information is stored and safeguarded. It is designed to protect personal information from unauthorised use or disclosure.

Principle six gives individuals the right to access information about themselves and also sets out the situations where such access may be refused.

Principle seven gives individuals the right to correct information about themselves and imposes a requirement on anyone who has disclosed inaccurate information to notify the recipients of that fact.

Principles eight to eleven place restrictions on how people and organisations can use or disclose personal information. A general rule is that information obtained for one purpose cannot be used or disclosed for another purpose except in specified situations.

Principle 12 governs how unique identifiers can be used.

The provisions of the Privacy Act are administered by the Privacy Commissioner. It provides for codes of practice that can become legally binding. One such code is the *Health Information Privacy Code 1994*[54], which was revised in 2008. 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.

6.3 National structures for information governance

In New Zealand the Ministry of Health, led by the Minister of Health, has overall responsibility for the health and disability system. The Ministry has a number of business units with specific areas of expertise that operate separately from it. One such business unit is the information directorate. The information directorate was formed in July 2008, taking over the responsibilities of two services that had previously been in place. At the time of writing of this document the directorate is still undergoing the transition phase and is continuing to review and revise processes.

Further reforms have also taken place recently in relation to the body with responsibility for health information standards. The Health Information Standards Organisation, established in 2003 was in 2005 renamed as the Health Information Strategy Action Committee (HISAC), revising the terms of reference accordingly. From 2005 until 2009 the Health Information Standards Sub-Committee formed part of HISAC. This was again reconstituted in 2009.

The national structures in place are as follows:

- The Ministry of Health
- The Health Information Standards Governance Group
- The Health Information Standards Office.

At the time of writing of this report there is limited information available on the Health Information Standards Governance Group and the Health Information Standards Office.

The terms of reference for the group are as of yet unavailable and as such it is unclear what will be their exact roles in relation to IG.

6.3.1 The Ministry of Health, New Zealand

The Ministry of Health works as policy adviser, regulator, funder and service provider. It works within the legislative framework set by the New Zealand Public Health and Disability Act 2000[55]. One area of responsibility is the governance of the health network.

The Health Network established in 2005 forms part of the national framework for the secure and private collection and sharing of electronic health information. It was designed to assist the delivery of integrated healthcare by enabling different health organisations to exchange information over a secure network. Information collected and shared includes patient laboratory results, discharge summaries and surgical notes. The Ministry of Health is responsible for the governance of the Health Network. These responsibilities include ensuring that appropriate standards, policies and procedures are in place. Security is of central importance in this regard. Users of the Health Network must be registered and comply with certification and security requirements for their local environments. Each member is subject to conformance checks against criteria contained in the *Health Network Code of Practice*.

The *Health Network Code of Practice* is based on New Zealand health and privacy legislation, industry principles for the protection of personal health information and the International Standards Organisation (ISO) information technology standards. Health Network members need to demonstrate that they have policies and procedures in place to address third party access, personnel security, physical and environmental security, systems development and maintenance and technical compliance as well as risk management for any security breach.

In line with this a *Security Policy for General Practitioners and other Health Professionals*[56] has been developed specifically relating to the health network. Within this policy it is recommended that all practices have a security policy implemented within their organisation. Recognising that many organisations may not have the resources or expertise to develop this, a generic security policy[57] has been developed. This generic security policy can be customised to suit a particular organisation. The generic security policy covers the following areas:

- general security policy and standards
- security organisation
- asset classification and control
- personnel security
- physical security

- computer systems access control
- New Zealand health network
- security in system life cycle management
- computer integrity and incident reporting
- malicious software
- business continuity management
- compliance.

6.3.2 The Health Information Standards Governance Group

The Health Information Standards Governance Group, established in 2009 reconstituted from sub-committees previously reporting to HISAC, is now the overarching governing body for health information standards in New Zealand. Its role is to:

- provide direction on the standards to be developed via HISO
- advise on, and recommend to the Ministry, the way forward in relation to these standards, their development, maintenance and implementation
- validate and endorse the standards once development is complete.

The terms of reference for the group are not yet available but its membership is comprised of the following New Zealand bodies:

- The Medical Council
- The Nursing Council
- Chief Medical Officers Forum
- District Health Board (DHB) Chief Information Officers (CIO) Forum
- Accident Compensation Corporation
- Primary Care Information Management Group
- Health Informatics New Zealand Executive
- NZ Health IT Cluster
- Ministry of Health (Chair).

It is anticipated that representation from these organisations will ensure continued sector participation and strong clinical leadership in the governance of health information standards. Although the terms of reference have not yet been specified as this is the body with responsibility for information standards it is likely that they will assume responsibility for IG.

6.3.3 The Health Information Standards Office

The Health Information Standards Office will support the Health Information Governance Group in its role by:

- providing secretariat services
- identifying relevant international standards for adoption or adaptation for use in New Zealand
- preparing proposals for required upgrades to existing health information standards and for the development of new health information standards
- facilitating and supporting the development of sector-wide standards for the group's validation and endorsement
- publishing endorsed standards
- advising the group about issues of standards compliance.

6.3.4 The Privacy, Authentication and Security (PAS) Framework

The New Zealand health sector has guidelines including the *Health Network Code of Practice*, *Health Information Privacy Code* and the *Health Intranet Policy* for the safe and secure electronic sharing of information. In the absence of a consolidated point of reference for security and privacy policies, the Ministry of Health is leading the development of a single consolidated guide for the sector in the form of a *Privacy, Authentication and Security (PAS) Framework* (see figure 2). The privacy and security protocols being developed under PAS are based on the *Health Network Code of Practice* and the *Health Information Privacy Code 1994* [(54)]. Security policies produced by the Health Intranet Governance Body were also used in the development of the protocols.

The *Health Network Code of Practice* was developed by Standards New Zealand in association with the Ministry of Health. It was the founding document for security within the health and disability sector.

The *Health Information Privacy Code 1994*[(54)], 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 substitutes for the information privacy principles in the Privacy Act. This code was published by the Office of the Privacy Commissioner.

The PAS protocols provide information and clarity that is relevant specifically in the health and disability sector to enable the following[(52)]:

- provide individuals and organisations in the health and disability sector with a set of protocols to enable the implementation of reasonable and appropriate privacy and security measures that balance costs, risks and the need to protect electronic health information
- avoid conflicting privacy and security approaches in current and planned electronic health implementations and allow organisations to take full advantage of the potential benefits of electronic health solutions

- establish consistent and coherent privacy and security practices across the health and disability sector, including standardising the roles and responsibilities for privacy and security, processes and appropriate technology
- increase the level of privacy and security coordination within the health and disability sector, including suppliers of technology and technology services, and other third-party suppliers who support the collection, use and exchange of electronic health information
- provide an authoritative reference point for organisations and individuals within the health and disability sector who intend to implement privacy and security measures to safeguard electronic health information
- provide guidance to management
- provide the foundation to create a culture of privacy and security awareness within the health and disability sector.

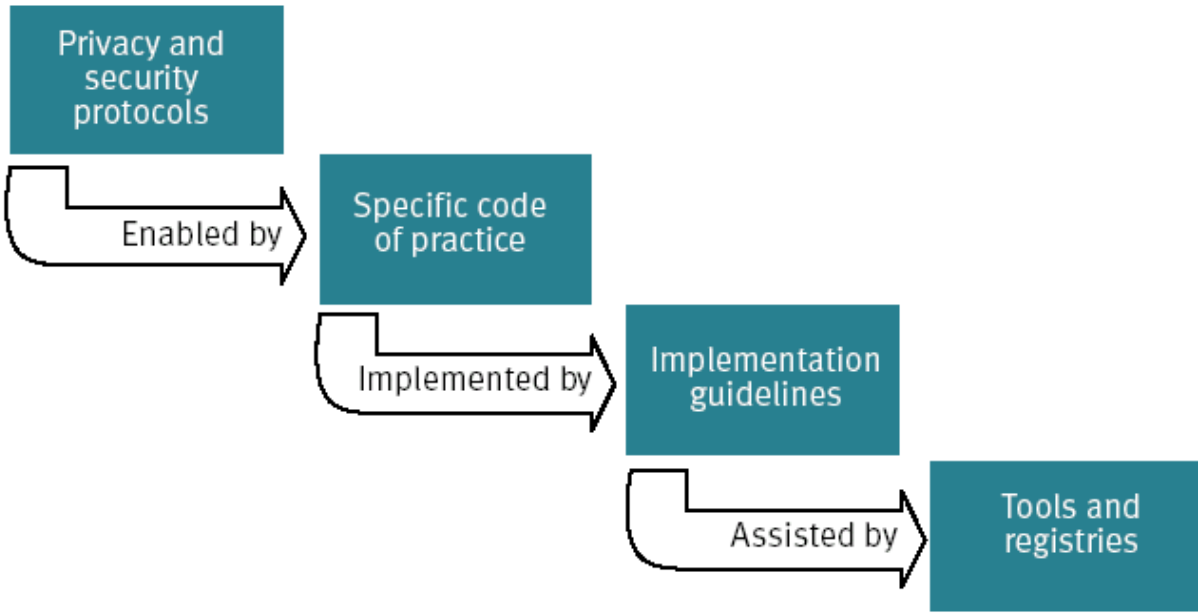


Figure 2: Privacy Authentication and Security (PAS) Framework

The PAS guide provides a number of key strategies; basing actions on these strategies is intended to ensure that trust is developed and maintained. These strategies include [52]:

- a specific code of practice for the sector
- a code of practice for each major participant involved in implementing or using information systems for the health sector
- practical implementation guidelines

- a self-assessment checklist for the sector and the implementation of a national register of systems that contain confidential patient data
- an approach to monitoring privacy and security compliance.

At the time of writing of this document the PAS project is in the process of being completed by the Ministry of Health. The PAS Framework will build on what is already in place and once developed will become the new standard.

6.3.5 Privacy regulation

At a provider level there are a number of sources of guidance available relating to IG. At the most basic level providers are required to comply with the principles as set out in the Privacy Act 1993. The associated *Health Information Privacy Code 1994*, (which is legally binding), sets specific rules for health sector agencies to ensure the protection of individuals' personal information. A revised copy of the code was issued in 2008 incorporating a number of amendments to the Privacy Act. These high level guidelines inform the development of policies, procedures and processes at an organisational level.

One such example is that of the National Immunisation Register (NIR) which published its *Privacy Policy*[58] in May 2004. The framework for the collection, exchange and management of health information about identifiable individuals held on the NIR falls within the provisions of the Privacy Act 1993[53] and the *Health Information Privacy Code 1994*[54]. The code, in particular, provides a broad framework of controls for the management of information about identifiable individuals.

Security guidelines are available in the form of the *Health Network Code of Practice* which requires compliance from providers if they are to be accepted as members of the network. The Ministry of Health has also made available a generic security policy that provides guidance to providers in terms of what is required of them.

The *Health Information Privacy Code* and the *Health Network Code of Practice* provide for IG requirements being met at a provider and organisation level.

6.4 Provider structures for information governance

At a provider level healthcare organisations can take guidance from the codes and policies outlined above, such as the *Health Information Privacy Code* and the *Security Policy for General Practitioners and other Health Professionals* developed by the Ministry of Health. However, at present, IG initiatives have not been developed at a provider level. This may change with the implementation of the PAS Framework which will require organisations to self-assess against a privacy and security code of practice.

6.5 Summary

The following significant developments in IG have taken place in New Zealand:

- the publication of the *Health Information Privacy Code* in 1994 and the updated version published in 2008
- the ongoing development of the *Privacy Authentication and Security Framework*, which will provide a single consolidated point of reference for healthcare providers in relation to IG
- the development of the *Health Network Code of Practice*.

The New Zealand model is one undergoing continued reform and it is likely that the next number of years will see further transformation and developments in respect of health IG.

7 Sweden

7.1 Overview

Sweden is a parliamentary democracy. The country is ruled by a government accountable to the Riksdag – the Swedish Parliament. It is the Riksdag which has legislative power in Sweden. The Swedish public sector has three levels of government; national, regional and local. At the local level, the entire territory of Sweden is divided into municipalities – each with responsibility for a broad range of facilities and services such as housing and water supply. At a regional level there are both elected county councils and county administrative boards. The county councils are responsible for overseeing tasks that cannot be handled at a local level and require coordination across a larger region, most notably healthcare. This decentralised system has led to mixed progress in eHealth and the adoption of national strategies, with each county and municipal council making independent decisions in respect of healthcare.

With regard to health information in Sweden the focus is currently, and has been for some time, on eHealth solutions and their implications. Many of the issues that arise however are similar to those that arise when handling and managing sensitive information in any format. The eHealth agenda has forced the Swedish Authorities to take a closer look at the way information is managed in terms of adopting a more collaborative national approach which is essential for the success of any national eHealth system.

A National eHealth Strategy(59) was published by the National High Level Group for eHealth[19] in March 2006, establishing a common vision of how eHealth should be used to support and improve healthcare. It is regarded as the first step in a long undertaking towards more cooperation on the national level. The strategy identified six areas of action as follows:

- bringing laws and regulation into line with extended use of ICT
- creating a common information structure
- creating a common technical infrastructure
- facilitating interoperable, supportive ICT systems
- facilitating access to information across organisational boundaries
- making information and services easily accessible to citizens.

These action areas will be explored in greater detail in the course of this section.

[19] This High Level Group was comprised of the Ministry of Health and Social Affairs, the Swedish association of Local Authorities and Regions, the National Board of Health and Welfare, the Medical Products Agency, the National Corporation of Swedish Pharmacies and Carelink.

The following are three priority areas that were identified as essential for the successful implementation of the strategy:

- organisational measures to facilitate exchanges of experience and collaboration on ICT tools that are of mutual interest
- information structure and standards for information documented within municipal health and social care
- technical infrastructure for secure login and communications based on digital identification.

Although the national strategy outlined above relates specifically to eHealth, it has implications for health IG on a broader scale. This is perhaps most apparent in terms of changes in legislation.

7.2 Legislation

The first of the six action areas identified in the National eHealth Strategy[59] was to bring laws and regulations into line with the extended use of ICT. This has been an area of early success in the form of the Patient Data Act 2008.

One of the primary obstacles to appropriate ICT use has been the failure of legislation and regulations to keep pace with development. The biggest issue has been to prevent unwarranted intrusion into patient privacy. An extensive review of the laws regulating this area is currently underway in the form of the Patient Data Inquiry in an attempt to harmonise laws and regulatory framework in the context of increased IT use.

In July 2008 the Patient Data Act entered into force replacing the Health Records Act and the Care Registers Act. The main point of departure has been to improve patient safety and privacy protection through the establishment of clear rules for how personal data can be handled securely and effectively. This represents a modernisation of the rules for how the health and medical services manage information about a patient. Under the new legislation, personnel in health and social care can digitally access a person's full history from care providers at different levels of the health care system. At the same time, it strengthens the framework for citizen influence and involvement as individuals themselves decide in a consent process who is to be given access to their overall record. Citizens will be able to access their own information electronically and see a log of which personnel have had access to their record[60].

7.3 National structures for information governance

The Swedish approach to IG has been fragmented to date but efforts are being made to rectify this through a number of projects that are underway at a national level as

outlined in the National eHealth Strategy[59]. The National Board of Health and Welfare has a role to play in health IG however the most significant developments will take place under the auspices of the six action areas identified in the National eHealth Strategy.

7.3.1 The National Board of Health and Welfare, Sweden

The National Board of Health and Welfare is the national expert body and supervisory authority in a range of policy areas including social services, public health protection, infectious disease control and health and medical care. The agency thus affects the actions of care professionals through its standardisation work, supervisory duties and knowledge communication initiatives. The Board has identified the legal, ICT-related and other conditions and requirements that must be met if the goals of “reliable, useful information on health and elderly care services, and easy, trouble-free access for citizens, fellow employees and decision makers” are to be met. The board was commissioned in its appropriation directions for 2006 to prepare to assume overall national strategic responsibility for ensuring that individualised patient data is more precisely formulated, accessible and capable of being followed up. This area of work is very much focused on data quality – a core component of IG. This requires a common national information structure, uniform classifications, nationally established quality indicators, and more rational and appropriate health care documentation procedures.

7.3.2 National eHealth Strategy - action areas and progress to date

The first action area of the Strategy has unquestionably been the most successful to date leading to the Patient Data Act 2008. The other action areas have resulted in a number of projects being undertaken, which at the time of writing of this report are at various stages of completion. The timelines for the completion of the majority of these projects is from 2009 to 2011. Table 2 details a sample of the projects underway under specific action areas and their relevance to IG issues[60].

Table 2: National eHealth Strategy action areas

Action Area	Rationale	Details of Project	Impact on IG
Creating a common information structure	The information handled in health and social care is a resource of long-term value and benefit. It will be made available to health and social care personnel and to the citizen for use as a basis for decisions, for management and follow-up activities for research. This is contingent on a national information structure that ensures that the correct information is documented and put into context.	The National Information Structure Project: This is intended to provide a basis for individualised, tailored health and care documentation, which can bring about more secure communication between actors with partly differing frames of reference and working in different units and functions.	This will have implications around security and the sharing of health information.
Creating a common technical infrastructure	A common and overarching technical infrastructure will facilitate communication, access and the sharing of sensitive information between involved and authorised actors. Citizen contacts with health and social care will also be simplified and personnel and managers in health and social care will have better access to national registers and databases to facilitate reporting and communications.	Standards for Electronic Interoperability in Health and Social Care Services: This service provides a body of regulation to create and interpret information so that it can be exchanged and used jointly by the health and social services without risk of misunderstandings. More reliable, clearer and more useful information improves patient safety and reduces resource consumption.	This has implications for the quality of information that is collected and used.
Facilitating interoperable, supportive ICT systems and facilitating access to information across organisational boundaries	ICT use varies across and within the organisations. The objective of ICT systems with good interoperability that allow the exchange or sharing of information, that are user-friendly for personnel and do not disturb the dialogue with patients, that provide information and knowledge support to safe and secure medical treatment, and can communicate with surrounding ICT systems.	The National Patient Summary: This project is designed to provide access to safer and more complete basic information for the care of patients, better opportunities for follow-up of care measures and lower costs for locating and reading important patient information. The service is intended to	The completion of this project will have implications around the way in which information is recorded, accessed and shared.

		facilitate access to important information about patients who have received care from other care providers, including other county councils and private providers, as well as the municipality. In the long term authorised care providers, with patient consent, will be able to locate and read relevant patient information, regardless of where it is in the country and what care sector it is.	
Making information and services easily accessible to citizens and personnel	Citizens will have easy and secure access to health and social care. They will be able to easily access health-related information, communicate in various ways with health and social care, and where needed, remain in continuous contact with their care providers. Increasing numbers of simpler services will be performed using ICT and ICT-supported telephone services.	The following priorities were identified and a number of supporting programmes have been put in place: ▪ to ensure that eHealth solutions can be used by all individuals or all ages regardless of physical or technical ability ▪ to enable citizens to examine information about their own care and health status via the same common access point.	This has implications around access to information and patient involvement in their care and the management of their information.

7.4 Provider structures for information governance

The projects outlined above will have implications for the governance of information by healthcare providers. At present the implications have not yet been realised but the completion of the provisions in the National eHealth Strategy will transform the way in which information is managed at a national and at a provider level.

7.5 Summary

Much of the work programmes resulting from the e-Health strategy are ongoing and due to be completed in the period 2009 – 2011. However the initiation of these projects in themselves represent significant development in IG in Sweden. A key area of early success is undoubtedly the 2008 Patient Data Act, representing a new departure in legislation and a modernisation of the rules for how the medical and health services manage information about a patient. Similar to the other countries explored, the focus in Sweden is on developing a more cohesive national approach to the management of information.

8 Conclusions

The aim of this document was to explore the international experience of IG to determine best practice. Legislation, national and provider structures and projects and initiatives that are currently underway in a number of countries were documented. Much of the IG work that is in progress relates to eHealth. This is the case in Canada, Sweden and Australia, with Australia and Sweden having recently developed eHealth strategies. However the same IG issues arise regardless of the format of the information.

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

- a structured national approach to IG - England and Scotland have developed a structured national approach with the others working towards this
- clear lines of accountability for IG at a national and local level, such as Caldicott Guardians in each healthcare organisation in England and Scotland acting as the "conscience" of that organisation.
- a central authority or point of reference on IG issues, for example the National Information Governance Board in England
- national standards and codes of practice for IG based on legislation, typically data protection and freedom of information legislation
- more specific policies and procedures developed at a provider level based on legislation and national codes of practice
- self-assessment tools and external audit to monitor compliance, such as the IG toolkit in England and Scotland.

At the time of writing of this report a number of developments are ongoing – most notably in Sweden and New Zealand. As such the information presented in this document may be superceded.

Prior to commencing the development of national standards for health IG, the Authority has sought to inform itself, through this review, of international best practice. The review also provides an opportunity to learn from instances where initiatives have not been successful. The review is the first step in a process that will inform the development of the standards.

Having completed this review the next step for the Authority is to undertake an "As Is" analysis of what already exists in Ireland. This will involve a review of relevant legislation, including the forthcoming Health Information Bill, IG policies and procedures that are already in place at a national level, and a series of meetings with stakeholders that have experience or an interest in the area.

The information detailed in the “As Is” analysis, in addition to that included in this report will inform the development of national standards for health IG. The development of these standards will be led by the Authority, which will also have a role in monitoring compliance against the standards, as per the provisions in the Health Act. This process will be informed by stakeholder consultation.

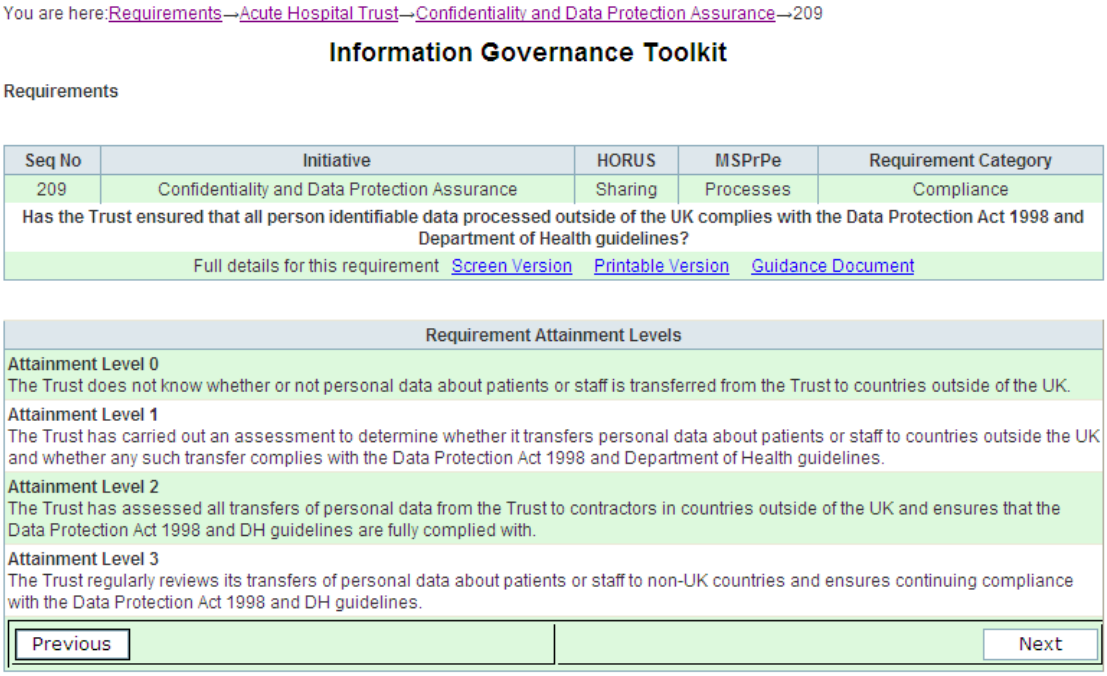
Appendices

Appendix 1
Acronyms

CEO	Chief Executive Officer
DoHC	Department of Health and Children
EHR	Electronic Health Record
EMR	Electronic Medical Record
HSE	Health Service Executive
ICT	Information and Communications Technology
IG	Information Governance
IM	Information Management

Appendix 2
IG Toolkit Acute Hospital 'View', Sample Requirement

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance



You are here:Requirements→Acute Hospital Trust→Confidentiality and Data Protection Assurance→209

Information Governance Toolkit

Requirements

Seq No	Initiative	HORUS	MSPrPe	Requirement Category
209	Confidentiality and Data Protection Assurance	Sharing	Processes	Compliance

Has the Trust ensured that all person identifiable data processed outside of the UK complies with the Data Protection Act 1998 and Department of Health guidelines?

Full details for this requirement Screen Version Printable Version Guidance Document

Requirement Attainment Levels
Attainment Level 0 The Trust does not know whether or not personal data about patients or staff is transferred from the Trust to countries outside of the UK.
Attainment Level 1 The Trust has carried out an assessment to determine whether it transfers personal data about patients or staff to countries outside the UK and whether any such transfer complies with the Data Protection Act 1998 and Department of Health guidelines.
Attainment Level 2 The Trust has assessed all transfers of personal data from the Trust to contractors in countries outside of the UK and ensures that the Data Protection Act 1998 and DH guidelines are fully complied with.
Attainment Level 3 The Trust regularly reviews its transfers of personal data about patients or staff to non-UK countries and ensures continuing compliance with the Data Protection Act 1998 and DH guidelines.

Previous Next

Reference List

Reference List

(1) Madden D. Empowering Health Information: Medico-Legal Issues. *Medico-Legal Journal of Ireland* 2002; 8(1).

(2) The Department of Health and Children. Discussion Document on Proposed Health Information Bill. June 2008. Available from: URL: http://www.dohc.ie/consultations/closed/hib/discussion_paper.pdf. Accessed: 28 Sep 2009

(3) The Department of Health and Children. *Quality and Fairness: A Health System for You*. 2001.

(4) The Commission on Patient Safety and Quality Assurance. *Building a Culture of Patient Safety*. 2008.

(5) The Department of Health and Children. Proposed Health Information Bill. 2009. Available from: URL: http://www.dohc.ie/issues/hib/. Accessed: 30 Sep 2009

(6) The Health Act 2007.

(7) The Department of Health and Children. *Health Information - A National Strategy*. 2004.

(8) NHS - Connecting for Health. Health and social care staff members: What you should know about Information Governance. 2008. Available from: URL: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/whatsnew/infogovleaflet.pdf. Accessed: 28 Sep 2009

(9) The Care Record Development Board. Information Governance in the Department of Health and NHS - the Cayton Report. 2006. Available from: URL: http://www.nigb.nhs.uk/about/publications/igreview.pdf. Accessed: 28 Sep 2009

(10) The Data Protection Act (UK) 1998.

(11) The Freedom of Information Act (UK) 2000.

(12) The Department of Health, UK. NHS Information Governance - Guidance on Legal and Professional Obligations. 2007. Available from: URL: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/codes/lglobligat.pdf. Accessed: 17 Aug 2009

(13) The National Information Governance Board U. NIGB for Health and Social Care Terms of Reference. 2008. Available from: URL: http://www.nigb.nhs.uk/papers/nigb_tor_v1.pdf. Accessed: 30 Sep 2009

(14) NHS - Connecting for Health. Information Governance Toolkit. 2009. Available from: URL: https://www.igt.connectingforhealth.nhs.uk/. Accessed: 30 Sep 2009

(15) NHS - Connecting for Health. Caldicott Guardians. 2009. Available from: URL: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/caldicott. Accessed: 28 Sep 2009

(16) The Information Commissioner's Office, UK. Privacy Impact Assessment Handbook - Version 2. 2009. Available from: URL: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html. Accessed: 14 Sep 2009

(17) Information Services Division, NHS Scotland. A Brief Guide to Information Governance. 2007. Available from: URL: http://www.shb.scot.nhs.uk/initiatives/informationgovernance/documents/V2Info-governance-guide-070122.pdf. Accessed: 18 Aug 2009

(18) NHS Quality Improvement Scotland. Clinical Governance and Risk Management: Achieving safe, effective, patient-focused care and services. 2007. Available from: URL: http://www.nhshealthquality.org/nhsqis/files/CGRM_NOV_OCT07.pdf. Accessed: 30 Sep 2009

(19) The Freedom of Information (Scotland) Act 2002.

(20) The Scottish Executive Health Department. NHS Code of Practice on Protecting Patient Confidentiality. 2003. Available from: URL: http://www.elib.scot.nhs.uk/SharedSpace/ig/Uploads/2008/Oct/20081002150659_6074NHSCode.pdf. Accessed: 18 Aug 2009

(21) The Human Rights Act Scotland 1998.

(22) The Infectious Disease (Notification) Act (UK) 1889.

(23) The Confidentiality and Security Advisory Group for Scotland (CSAGS). Protecting Patient Confidentiality. 2002. Available from: URL: http://www.sehd.scot.nhs.uk/publications/ppcr/ppcr.pdf. Accessed: 17 Aug 2009

(24) NHS Scotland. Managing Patient Identifying Data: Best Practice Guidelines. 2003. Available from: URL: http://www.isdscotland.org/isd/servlet/FileBuffer?namedFile=ISD_anon_guide.pdf&pContentDispositionType=inline. Accessed: 18 Aug 2009

(25) NHS Scotland. Anonymisation and NHS Scotland National Data Sets. 2003. Available from: URL: http://www.isdscotland.org/isd/servlet/FileBuffer?namedFile=ISD_anon_report.pdf&pContentDispositionType=inline. Accessed: 18 Aug 2009

(26) The Scottish Executive Health Department. The Caldicott Guardian Manual 2007 - Scottish Version. 2007. Available from: URL: http://www.elib.scot.nhs.uk/SharedSpace/ig/Uploads/2007/Jun/20070627162905_UK%20Council%20of%20Caldicott%20Guardians%20Manual%20(Scotland%20version)_v1.6_2007.pdf. Accessed: 18 Aug 2009

(27) The Scottish Executive Health Department. The NHS Scotland Information Security Policy. 2006. Available from: URL: http://www.sehd.scot.nhs.uk/mels/HDL2006_41.pdf. Accessed: 18 Aug 2009

(28) The Scottish Government. Records Management: NHS Code of Practice. 2008. Available from: URL: http://www.scotland.gov.uk/Resource/Doc/230203/0062364.pdf. Accessed: 18 Aug 2009

(29) NHS National Services Scotland and NHS Education for Scotland. Information Governance in NHS Scotland: A Competency Framework. 2008. Available from: URL: http://www.nhsgrampian.org/grampianfoi/files/NES_Information_Governance_CompFramework.pdf. Accessed: 21 Aug 2009

(30) Personal Health Information Protection Act (Ontario) 2004.

(31) The Privacy Act (Canada) 1985.

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

(33) Canada Health Infoway. White Paper on Information Governance of the Interoperable Electronic Health Record (EHR). 2007. Available from: URL: http://www2.infoway-inforoute.ca/Documents/Information%20Governance%20Paper%20Final_20070328_EN.pdf. Accessed: 28 Sep 2009

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

(35) British Columbia Ministry of Labour and Citizens' Services. PIPA Tool: Ten Principles for the Protection of Privacy. 2003. Available from: URL: http://www.mser.gov.bc.ca/privacyaccess/Privacy/Tools/PIPA_Tool_4.htm. Accessed: 28 Sep 2009

(36) College of Physicians of Alberta Medical Informatics Committee. Data Stewardship Framework. December 2006. Available from: URL: http://www.cpsa.ab.ca/Libraries/Res/CPSA_Data_Stewardship_Framework.sflb.ashx. Accessed: 21 Aug 2009

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

(38) The International standards Organisation. *ISO 17799 Security Standard*. 2005.

(39) Ontario Hospital Association. *Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals*. 2003.

(40) Freedom of Information and Protection of Privacy Act (British Columbia) 1996.

(41) Health Authorities Act (British Columbia) 1996.

(42) National Health Information Management Principal Committee. Strategic Work Plan 2007-08 to 2012-13. 2007. Available from: URL: http://www.ahmac.gov.au/NHIMPC_Strategic_Work_Plan.pdf. Accessed: 29 Sep 2009

(43) The National eHealth Transition Authority. Privacy Blueprint - Unique Healthcare Identifiers. 2006. Available from: URL: http://www.nehta.gov.au/index.php?option=com_docman&task=doc_view&gid=148&Itemid=139. Accessed: 5 Oct 2009

(44) 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. Available from: URL: http://www.dohc.ie/consultations/closed/hib/draft_audit_paper.pdf?direct=1. Accessed: 24 Aug 2009

(45) The Privacy Act (Australia) 1988.

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

(47) The Australian Institute of Health and Welfare. Health Sector Reporting Relationships for Health Committees. 2008. Available from: URL: http://www.aihw.gov.au/committees/nhissc/index.cfm. Accessed: 30 Sep 2009

(48) The Australian Institute of Health and Welfare. Australia's Health 2008. 2008. Available from: URL: http://www.aihw.gov.au/publications/aus/ah08/ah08.pdf. Accessed: 29 Sep 2009

(49) The Department of Health and Ageing, Australia. The Regulation of Health Information Privacy in Australia. 2004. Available from: URL: http://www.nhmrc.gov.au/PUBLICATIONS/synopses/_files/nh53.pdf. Accessed: 27 Aug 2009

(50) Office of the Federal Privacy Commissioner, Australia. Guidelines on Privacy in the Private Health Sector. 2001. Available from: URL: http://www.privacy.gov.au/materials/types/guidelines/view/6517. Accessed: 27 Aug 2009

(51) The Wave Advisory Board to the Director-General of Health. From Strategy to Reality: the WAVE Project. 2001. Available from: URL: http://www.moh.govt.nz/moh.nsf/0/F34F8959738E992CCC256AF400177998/$File/TheWAVEreport.pdf. Accessed: 28 Sep 2009

(52) Health Information Strategy Steering Committee, New Zealand. Health Information Strategy for New Zealand. 2005. Available from: URL: http://www.moh.govt.nz/moh.nsf/0/1912064EEFEC8EBCCC2570430003DAD1/$File/health-information-strategy.pdf. Accessed: 29 Sep 2009

(53) The Privacy Act (New Zealand) 1993.

(54) The Office of the Privacy Commissioner, New Zealand. The Health Information Privacy Code 1994 - Revised Edition. 2008. Available from: URL: http://www.privacy.org.nz/assets/Files/Codes-of-Practice-materials/HIPC-1994-2008-revised-edition.pdf. Accessed: 24 Aug 2009

(55) New Zealand Public Health and Disability Act 2000.

(56) The Ministry of Health, New Zealand. New Zealand Health Network of New Zealand - Security Policy for General Practitioners and other Health Professionals. 2006. Available from: URL: http://www.moh.govt.nz/moh.nsf/pagesmh/8805/$File/NZHNsecurity.pdf. Accessed: 26 Aug 2009

(57) The Ministry of Health, New Zealand. Generic Security Policy - For the Small Practice. 2005. Available from: URL: http://www.moh.govt.nz/moh.nsf/pagesmh/8806/$File/genericsecurity.doc. Accessed: 26 Aug 2009

(58) The National Immunisation Register, New Zealand. Privacy Policy - Setting out the Management of Health Information contained in the National Immunisation Register. 2004. Available from: URL: http://www.moh.govt.nz/moh.nsf/pagesmh/6693/$File/privacy-policy-nir.pdf. Accessed: 27 Aug 2009

(59) National High Level Group for eHealth, Sweden. National Strategy for eHealth, Sweden. 2006. Available from: URL: http://www.regeringen.se/content/1/c6/06/43/24/f6405a1c.pdf. Accessed: 5 Oct 2009

(60) The Ministry of Health and Social Affairs, Sweden. Swedish Strategy for eHealth. Safe and accessible information in health and social care. Status Report 2009. 2009. Available from: URL: http://www.sweden.gov.se/sb/d/2028/a/124802. Accessed: 3 Sep 2009

For further information please contact:

Health Information and Quality Authority

Unit 1301, City Gate,
Mahon,
Cork

T: +353 21 240 9300
E: info@hiqa.ie
URL: www.hiqa.ie