An "As Is" Analysis of Information Governance in Health and Social Care Settings in Ireland

January 2010

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, personal information 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)]. As a result, the development of national standards and guidelines 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 forms- 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 responsibility under the Health Act for the development of standards and monitoring against these in respect of health information. As such, the Authority has a key role to play in developing and monitoring standards for IG in the health and social care system in Ireland.

The need for an IG framework has been reiterated since it was first recommended in the Government's 2001 document *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*[(4)], the 2008 *Report of the Commission on Patient Safety*[(5)] and the *Draft Health Information Bill*[(6)].

The importance of IG in healthcare settings has been well documented but, at present, the system is fragmented and lacks a cohesive structure that would enable the benefits to be realised and provide the safeguards required 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, quality of care and the health service generally.

[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, the Authority and healthcare providers (both public and private) each have a role to play in developing and implementing national standards for health IG for Ireland's health and social care system. The Health Information Inter-Agency Group was established in April of 2008. Membership is comprised of representatives from Department of Health and Children, the Authority and the Health Service Executive (HSE). The group was established to facilitate cooperation and coordination of work by these three bodies in the area of health information. One of the primary objectives of the group was to clarify the respective roles of each of its members. In relation to national standards for health IG roles have been agreed as follows:

- 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 under the Health Act
- the HSE has responsibility for the implementation of the approved standards

The 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 Health Information and Quality Authority as set out in the Health Act 2007 is outlined as follows(7):

> **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(4). The report states, within this action, a specialist function

[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.

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 key stakeholders.

The purpose of this document is to examine and outline the legislative provisions relating to IG and the structures, alongside policies and guidelines that are in place in the Irish health and social care sector. This document, in addition to the Authority's *International Review of Information Governance Structures*[8] will inform decision-making on how best to approach the development and monitoring of national standards for IG in the Irish health and social care sector.

Table of Contents

1 Introduction

Action 18 of the *National Health Information Strategy 2004* calls for the development of a framework for IG[4]. The strategy states, within this action, that a specialist function for IG will be established by the Authority. In line with this, and the provisions in the Health Act, 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 and outline the legislative provisions relating to IG along with the structures, policies and guidelines that are in place in the Irish health and social care sector. This document, in addition to the Authority's *International Review of Information Governance Structures*[8] will inform decision-making on how best to approach the development and monitoring of national standards for IG in the Irish health and social care sector.

1.1 What is Information Governance?

According to the *National Health Information Strategy*[4] 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".

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, IG enables organisations to put in place processes and procedures 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 assist compliance with corporate governance standards[9].

In order to bring coherency, transparency and assurance to information initiatives in health and social care settings, an IG framework is required. The framework can be broadly covered under the following six areas:

- IG management. This refers to having an appropriate management structure in place to support an IG framework for organisations. Dedicated staff members should have a responsibility for the management

of IG within an organisation and all staff members should be adequately informed and trained of their responsibilities in this regard[10]

- confidentiality and data protection assurance. This element is driven by the requirements of the Data Protection Acts 1988 and 2003[11;12] which require that the processing of personal information should be carried out confidentially in health and social care settings. Patients and service-users should be adequately made aware of their choices with regard to the sharing of their information[10]

- information security assurance. This relates to having systems in place that ensure that all information is held confidentially and securely, can be relied upon in use, and is available to authorised persons when and where needed[10]. It is concerned not only with technical methods for securing information but also deals with physical security measures

- clinical information assurance. This is concerned with ensuring the accuracy of records so that healthcare professionals can be confident that care decisions are based on reliable, high-quality information. This work area is also concerned with procedures being in place to ensure the availability of records when and where they are required

- secondary use of information assurance. This is concerned with ensuring the appropriate use of information collected for secondary purposes such as research and clinical audit, while protecting the rights of the patient concerned

- freedom of information assurance. This element is driven by the requirements of the Freedom of Information Acts 1997 and 2003[13;14]. It seeks to ensure that organisations implement measures to comply with the timescales for responding to an information request. It also requires an appropriate records management policy and the identification of staff members who are accountable for FOI in each organisation.

1.2 Methodology

This document focuses on identified areas of good practice and provides an overview of the guidance that is in place at a national level in respect of IG. To avoid unnecessary duplication this document does not present an exhaustive review of work previously undertaken but instead focuses on provisions already in place as a starting point to inform the development of national guidelines for health IG.

Section two of this document reviews the national and European legislation in addition to other legal considerations that contain provisions relating to IG.

The document then focuses on how IG is managed within the health and social care settings in Ireland. It identifies what has been developed in relation to guidelines, policies and codes of practice under the headings of:

- confidentiality and data protection assurance
- information security assurance
- clinical information/care records assurance
- secondary use assurance
- freedom of information assurance.

In order to complete this work, the Authority consulted with a range of stakeholders and met with representatives of the following bodies (see Appendix 2):

- the Department of Health and Children
- Health Intelligence Unit (Population Health), HSE
- the National Cancer Registry, Ireland
- the Office of the Data Protection Commissioner
- the Centre for Management and Organisation Development
- the Health Research Board
- the Irish College of General Practitioners and the National GPIT Group
- the HSE Information Governance Board
- the HSE Information Governance Project Team
- An Bord Altranais
- the Office of the Information Commissioner
- the Central Statistics Office.

2 Legislation

National standards and guidelines for health IG will be based on existing national and international legislation. Nationally, there are a number of Acts that impact on the handling and management of information, both general and health-specific. Of these, the Data Protection and the Freedom of Information Acts[11-14] are to the fore, pending the enactment of the forthcoming Health Information Bill. There are a number of other Acts containing specific provisions relating to the management of information that also warrant consideration.

This section documents the legislative considerations surrounding IG under the following headings:

- the Constitution
- national legislation
- international legal considerations.

2.1 The Constitution

Although there is no express reference to a right to privacy in the Irish Constitution, the Supreme Court has ruled that an individual may invoke the personal rights provision in Article 40.3.1 which establish an implied right to privacy. Specifically, Article 40.3.1 states[15]:

> "The State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizen."

2.2 National legislation

Provisions relating to IG are evident in many pieces of national legislation such as:

- the forthcoming Health Information Bill
- Data Protection Acts 1998 and 2003
- Data Protection (Access Modification) (Health) Regulations 1989
- Freedom of Information Acts 1997 and 2003
- The Health (Provision of Information) Act 1997
- The Disability Act 2005
- The Statistics Act 1993
- The Social Welfare Acts 1998 and 2002
- The European Convention on Human Rights Act 2003.

2.2.1 The Health Information Bill

The 2001 report by the Department of Health and Children – *Quality and Fairness, A Health System for You* [3] – specifies that the Department of Health and Children will publish a Health Information Bill[6] which will aim to put health IG on a sound and robust footing and provide a clear legislative context for supporting health service professionals while recognising the rights and duties of service-users, health professionals and health agencies.

This will provide a set of rules to ensure full and proper use of information while protecting the privacy of the individual. The Department of Health and Children published a *Discussion Document on the Health Information Bill* in June 2008[2]. According to this document, the aim of the Bill is to enable information to be used to enhance medical care and patient safety through the use of information technology. In order to do this, the Bill will define the legislative framework to underpin an effective IG structure for the health system generally. It is expected that the Bill will build on existing legislation such as the Data Protection and Freedom of Information Acts. Once enacted, this legislation will form the legal basis for the national health IG standards and guidelines. At the time of writing this report the Bill is in the process of being drafted with an anticipated date of enactment of mid-2010.

2.2.2 The Data Protection Acts 1988 and 2003

In 1988, the Data Protection Act[11] was passed in order to implement the 1981 Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data[16]. The Act regulates the collection, processing, keeping, use and disclosure of computerised personal information relating to living identifiable individuals. It covers both the private and public sectors. Unlike the data protection regimes in a number of other European countries, the Act did not initially extend to information on manual files, but was subsequently amended in 2003 to include manual files and to implement the EU Data Protection Directive of 1995. The Data Protection Act of 2003 strengthened individuals' rights (as data subjects) in relation to their personal information and imposed more obligations on those who keep such information (data controllers). The Data Protection Act of 2003 also extends data protection law to manual records and introduces special provisions in relation to categories of sensitive information, including personal health information[17].

The eight principles of Data Protection as outlined in the Act dictate that personal information be[18]:

- obtained and processed fairly, which means that the person providing it knows the purposes for which it will be used and the persons to whom it will be disclosed
- relevant and not excessive
- held no longer than is necessary
- devoid of prejudicial, derogatory, malicious, vexatious or irrelevant statements about the individual
- purpose specific
- held securely
- accessible to the individual or person acting on his or her behalf on a reasonable basis.

These principles, when applied in the healthcare setting relate to:

- using, disclosing and transferring personal health information
- patient consent to collecting information
- patient access to personal health information.

These provisions, when interpreted to apply to health and social care settings, envisage patient data being processed by a data controller[3]. This would include research contexts where the processing is undertaken by a health professional or other person owing a similar duty of confidentiality to that patient, providing this is done in a manner that protects the rights and freedoms of the patient. This can mean either the data being anonymised or the individual in question giving consent for their data being used for specified research purposes.

The Act also provides an exemption from obtaining consent in cases where the data is to be processed for statistical, research or scientific purposes by the data controller and where there are no disclosures of personal data to any outside, third parties. In this instance, the data will not be considered to have been unfairly obtained, as long as no damage or distress is likely to be caused to an individual. In relation to data in healthcare settings, best-practice suggests that allowing the patient choice and providing them with information in relation to how their data is used should be the standard approach(19).

The Data Protection Commissioner has statutory responsibility for implementing the terms of the Data Protection Acts and has a wide range of powers which can legally oblige a person holding personal data to comply with the terms of the Acts. These powers include the requirement for a person to provide information needed to assist with enquiries being carried out by the Office of the Data Protection Commission and restrict the transfer of information abroad. The Data Protection Commissioner is responsible for upholding the rights of individuals as

[3] A data controller is the individual or the legal person who controls and is responsible for the keeping and use of personal information on computer or in structured manual files.

set out in the Acts, and enforcing the obligations upon data controllers. The Commissioner is appointed by the Government and is independent in the exercise of his or her functions. Individuals who believe that their rights in relation to their personal data are being infringed, can complain to the Commissioner, who will investigate the matter, and take whatever steps may be necessary to resolve it[20].

One of the core functions of the Office of the Data Protection Commissioner is to ensure compliance with the provisions of the Data Protection Legislation. To this end, the Office of the Data Protection Commissioner has been conducting compliance audits, including audits of healthcare facilities, against Data Protection legislation since 2003. A compliance audit typically examines an organisation's procedures, policies, systems and records in order to assess whether the organisation is generally in compliance with the provisions of data protection legislation[21]. Once an audit has been completed, an audit report and resulting recommendations are published on the website of the Office of the Data Protection Commissioner (www.dataprotection.ie).

As part of the audit process an examination takes place of the categories of information being sought as part of the patient registration process. This is to ensure that healthcare facilities are authorised to request and process data, for example the use of the Personal Public Service (PPS) Number. The audit also includes an examination of access rights to both electronic systems and manual files that contain personal information. The requirement to have a retention policy in place for all categories of personal data is also part of the audit. General security requirements also feature in the audits and involve ensuring that satisfactory safeguards regarding physical and electronic security procedures are in place, including, when required, the secure destruction of manual and electronic files that contain personal information.

2.3.2 Data Protection (Access Modification) (Health) Regulations 1989

These regulations prohibit the supply of health data to a patient in response to a request for access in the case that such access would cause serious harm to his or her physical or mental health. This legislation also makes the provision that such data is to be communicated only by, or after consultation with, an appropriate "health professional" — normally the patient's own doctor[22].

2.3.3 The Freedom of Information Acts 1997 and 2003

The Freedom of Information Act 1997[13], as amended by the Freedom of Information Act 2003[14], grants individuals the legal rights to access both

personal and non-personal information and to have their personal information amended if it is inaccurate. The Office of the Information Commissioner has been established to review decisions by, and practices of, public bodies in addition to the operation of the Acts[23].
The Freedom of Information Acts 1997 and 2003 apply to public bodies and give individuals the legal right to[2]:

- access both personal and non-personal (organisational and corporate) records
- have personal records amended or deleted where the information is incorrect, incomplete or misleading
- seek reasons for decisions that affect them.

Information about the activities of public bodies covered by the Freedom of Information Act (Sections 15 and 16) is contained in the Freedom of Information Manual, which every public body is obliged to publish.

The main functions of the Information Commissioner, as set out in the Act, can be summarised as follows:

- reviewing (on application) decisions of public bodies in relation to FOI requests and where necessary, reverse the decision made by the public body
- reviewing the operation of the Freedom of Information (Amendment) Act, 2003 to ensure that public bodies comply with their provisions
- fostering an attitude of openness among public bodies by the encouragement of the voluntary publication of information above and beyond the minimum requirements of the Acts
- the preparation and publication of commentaries on the practical operation of the Acts
- the publication of an annual report.

Freedom of Information (FOI) legislation does not apply to the private sector. For example, private hospitals and general practitioner (GP) practices are not covered by the relevant Acts. However, where a private entity is providing services to the public sector for example, GPs providing services to medical card patients, then FOI legislation applies.

Given that FOI legislation makes provision for service-users to access their health records and have personal records amended or deleted where the information is incorrect, incomplete or misleading, this has had an impact on the way in which health and social care organisations manage their records and deal with FOI requests.

The main similarities and differences between the Data Protection and Freedom of Information Acts are outlined in appendix three.

2.3.4 Health (Provision of Information) Act 1997

Cancer Services in Ireland: A National Strategy[24], published in 1996, outlined the proposed details for breast and cervical cancer screening programmes including a number of the information management requirements of such programmes. Screening programmes such as those proposed can only operate effectively if population registries containing the names and addresses of women in the target age group can be established and regularly updated. Specific legislation, the Health (Provision of Information) Act 1997, was required in support of the proposed screening programmes as the disclosure of personal information necessary to compile these databases was in contravention with the provisions of data protection legislation[25]. The Data Protection Commissioner (in his Annual Report for 1997)[26] stated that the Health (Provision of Information) Act:

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

The Health (Provision of Information) Act 1997 allows for the provision of information to the National Cancer Registry Board, the Minister for Health and certain other health bodies, for the purposes of cancer screening programmes, and to provide for related matters[27].

The National Cancer Registry is subject to Data Protection legislation in terms of how information is managed, stored and used. As a result, the National Cancer Registry of Ireland (NCRI) has very clearly set out its legal and ethical position on preserving confidentiality in its document *Data Confidentiality in the National Cancer Registry* [28].

One of the key issues for consideration in the drafting of the Health Information Bill is what principles should guide the development and regulation of National Health Population Registers, such as that of the National Cancer Registry, and the instances in which reporting to such registers should be mandatory[2].

2.3.5 Disability Act 2005

The Disability Act[29] is designed to advance and underpin the participation of people with disabilities in society by supporting the provision of disability specific

services and improving access to mainstream public services. The Act includes a number of provisions relevant to IG.

Part 2, Section 12 of the Act relates to the exchange of information between service providers and healthcare professionals. Within this section there is a provision for informing, with the necessary consent of the person concerned, other service providers about the contents of an assessment report so as to facilitate access to services outside the health and education sectors[30].

Part 4 of the Act relates to genetic testing. It provides safeguards for the use of information obtained from genetic testing. The provisions aim to ensure that people who may be affected by genetic disorders will not be subject to any unreasonable personal information requirements from an employer or an insurance or mortgage provider. The protections provided are in addition to the substantial safeguards for the use of personal information contained in the Data Protection Acts[11;12]. Part 4 of the Act states that[30]:

- genetic testing may only take place with a person's consent, in accordance with the Data Protection Acts
- the results of a genetic test cannot be used in relation to insurance, a mortgage, a personal pension or employment
- the person being tested must be made aware of the intended use of the test results and must, as far as possible, be informed about the possible outcomes of the test.

2.3.6 Statistics Act 1993

The Statistics Act, 1993[31] provides the legislative basis for the compilation and dissemination of official statistics. The Act came into effect on 1 November 1994. This legislation provides a statutory basis for the collection and use of specified information, including personal health information and allows for outside parties to be designated, under the Act, for the purposes of carrying out certain research on the information collected[25].

The Act officially established the Central Statistics Office (CSO). The CSO is an independent office under the aegis of the Department of An Taoiseach to guarantee statistical independence and the confidentiality of the data it collects. The functions of the Office are "the collection, compilation, extraction and dissemination for statistical purposes of information relating to economic, social and general activities and conditions in the State"[31]. Part 3 of the Act deals with the collection of information and invokes the provisions contained in the Data Protection Act, 1988[11]. Part 5 relates specifically to the protection of information.

Under the Act the CSO is permitted to collect personal information. For example, the CSO collects and registers information about births and deaths of individuals. They also collect information on health and social conditions, for example generating statistics on acute hospital services and on disability, carers and voluntary activities.

2.3.7 Social Welfare Acts 1998, 2002 and 2005

The Social Welfare Act 1998[32], as well as introducing the Personal Public Service (PPS) Number as being obligatory for the receipt of publicly funded services, also introduced the concept of a Public Service Card[25]. The PPS Number replaced the Revenue and Social Insurance (RSI) number, which for years, was used for social welfare and tax purposes only. The Act allows for the exchange of personal data between specified bodies in certain circumstances, and its provisions are expressly exempt from the Data Protection Act. The Act makes it an offence for anyone other than a State Agency to attempt to obtain an individual's PPSN.

According to the Act "specified body" means[32]:

- a Minister of the Government
- a Local Authority
- The Revenue Commissioners
- The Health Service Executive
- Foras Aiseanna Saothair (FAS)
- An Post
- An tArd-Chlaraitheoir
- The Legal Aid Board
- The Mental Health Commission
- The Garda Siochana and the Defence Forces in respect of their own members or
- other such persons as may be prescribed.

The HSE, for example, uses the PPS number to assist in the identification process for medical card applications.

The Social Welfare and Pensions Act 2005[33] extended the legal provisions relating to the use of the PPSN to include the Mental Health Commission, which as a result, was added to the list of "specified bodies". The Mental Health Commission records the PPS Number of each resident in an approved mental health centre as part of the data set collected in a register of residents.

The Social Welfare (Miscellaneous Provisions) Act 2002 further extended the provisions of the PPSN, introducing the concept of a public service identity card[34].

2.3.8 European Convention on Human Rights Act 2003

The European Convention on Human Rights Act, 2003[35], amends the Human Rights Commission Act, 2000[36]. It also gives further effect, subject to the Constitution, to certain provisions of the Convention for the Protection of Human Rights and Fundamental Freedoms 2003[37]. Article 8 of the Act deals with the right to respect for private and family life as follows[35]:

> **8** (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> **8** (2) There shall be no interference by a public authority with the exercise of this right except such as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The EU Data Protection Directive 1995[38] provides a common European framework for data protection. It is based on the twin pillars of respect for the fundamental right to privacy. The Directive limits the extent to which domestic legislation can infringe the individual's right to data privacy. This right is further reinforced by the domestic applicability of the European Convention on Human Rights and the related jurisprudence of the European Court of Human Rights, in accordance with the European Convention on Human Rights Act, 2003.

2.3.9 The Nurses Act 1985

The Nurses Act 1985[39] provides for the establishment of An Bord Altranais, the Nursing Board, to "provide for the registration, control and education of nurses" and other matters relating to the practice of nursing.

With regard to IG, Part 5 of the Act is of most relevance as it deals with fitness to practice. An Bord Altranais has published a number of documents providing guidance to nurses and midwives in relation to how information should be managed, for example, *The Code of Professional Conduct for each Nurse and Midwife*[40], and *Guidance to Nurses and Midwives Regarding Ethical Conduct of Nursing and Midwifery Research*[41].

2.3.10 The Medical Practitioners Act 1978 and 2007

The Medical Practitioners Act 1978[42] was enacted to provide for the establishment of the Medical Council. The roles of the Medical Council include:

- assuring the quality of undergraduate education of doctors
- assuring the quality of postgraduate training of specialists
- registration of doctors
- disciplinary procedures
- guidance on professional standards/ethical conduct
- professional competence.

In relation to their role in guidance on professional standards and ethical conduct the Medical Council published a *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*[43] in November 2009. This is the seventh edition of the guide.

The purpose of the Medical Practitioners Act 2007[44] is to better protect and inform the public in its dealings with medical practitioners. Part 6 of this Act relates to the registration of medical practitioners, with section 43 specifying provisions relating to the register of medical practitioners. Section 43 specifies that:

> **43** (8) A registered medical practitioner shall, as soon as may be after the person has received the certificate referred to in *subsection (5),* cause the registration number stated on that certificate to be included on all medical prescriptions and all other documentation and records, whether in paper or electronic format, relating to that practitioner's practice as a registered medical practitioner.

In addition to the provisions discussed above, medical practitioners also owe a duty of confidentiality to their patients, which is not provided for legislatively but is a feature of common law. Confidentiality underpins the professional-patient relationship although there is no specific legislative provision governing this duty of confidence. The obligation of confidence owed by a healthcare professional is governed by the rules of professional ethical conduct applicable to the profession and by the common law doctrine of confidentiality.

The common law duty of confidentiality affords some protection to a person in respect of the disclosure or use by another of information relating to that person. An action for breach of confidence is essentially a civil remedy affording protection against the disclosure or use of information which is not publicly known and which has been entrusted to a person in circumstances imposing an obligation not to disclose or use that information without the authority of the

person who has imparted it. There is, however, some uncertainty as to the precise nature and scope of this remedy. Apart from the ethical dimension, medical confidentiality could also arise from possible contractual obligations resulting from the professional-patient relationship, duties arising from the constitutional right to privacy, and equitable duties imposed by virtue of the relationship and nature of the information disclosed[2].

The confidential nature of a patient's healthcare information and the healthcare professional's obligation to respect that confidentiality are not changed by the death of the patient. A competent patient can give or withhold consent to disclosure before their death and such wishes should be respected as they would in other circumstances. In particular, where a competent patient has made an explicit request before his or her death that their confidence be maintained following requests from family members or carers for disclosure, then that request should normally be respected. However, the confidentiality requirement is not absolute and exists within a wider social context in which healthcare professionals have other duties, which may conflict with – and override – their duty of confidentiality. Medical practitioners are bound by a duty which the law respects from disclosing without the consent of the patient or client communications or information obtained in a professional capacity, save in certain situations; for example, where a disclosure is required under a particular statutory provision or a court order or where there is a serious or immediate threat to the health or life of another person[25].

2.4 International legal considerations

There is a range of international declarations, treaties and agreements relevant to the area of protecting the privacy and confidentiality of health information. Some cover the area of privacy and human rights generally whereas others are more specifically concerned with information privacy[25]. With regard to the more general area of privacy and human rights this has been encapsulated in the European Convention on Human Rights Act 2003[35], as outlined above.

With specific regard to data protection, the two major – and broadly similar – international data protection instruments are:

- *Organisation for Economic Cooperation and Development's Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data*[45]
- *Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*[16].

Both of these address information privacy issues in the context of the economic value associated with the free-flow of information across national borders. This also arises in the subsequent 1995 EU Directive on Data Protection[38] which was concerned with completing the Internal Market as regards the free flow of information between member states as well as raising the floor of privacy rights across the Union. Further, in both the Convention and the Directive, personal health information is identified as sensitive and therefore deserving of additional protection[25].

2.5.1 EU Data Protection Directive 1995

Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" is more widely referred to as the *EU Data Protection Directive*[38]. It was developed in the context of creating the infrastructure necessary for the completion of the internal market. It set a baseline common level of privacy in EU member states. This not only re-enforced existing data protection law, but extended it to establish a range of new rights for individuals (data subjects) such as improved rights of access and correction, a new right to block certain uses of information. It also imposed additional obligations on those collecting, holding, using, disclosing and transferring abroad personal information (data controllers). The purpose of the Data Protection Act 2003[12] was to implement the Directive in Ireland[25].

Article 8 of the Directive deals with the processing of special categories of data. Health information is expressly recognised as one of the sensitive categories. Member states must prohibit the processing of those special categories of data, except in the situations where [38]:

- the data subject has given his or her explicit consent
- the processing is necessary to protect the vital interests of the data subject or of another person
- the data subject is physically or legally incapable of giving consent
- the processing of the data is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy, or
- subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions either by national law or by decision of the supervisory authority.

2.6 Summary

There are a number of pieces of legislation that have relevance and include provisions for the collection, processing and management of information. A number of these are health-specific such as the Health (Provision of Information) Act 1997[27], while others such as the Data Protection Acts[11;12] are more generic. The legislation that is in place has informed the development of a number of guidelines, policies and processes, as detailed in sections three to eight of this paper. The implementation of the Health Information Bill, anticipated to be in 2010, will mark a new departure in IG in that it relates specifically to health information. The Bill is expected to build on the legislation that is already in place and seen to be working well – primarily the Data Protection and Freedom of Information Acts[11-14]. As such the Health Information Bill will form the legislative basis for the national health IG standards and guidelines to be developed by the Authority.

3 Information governance management

In order for an IG framework to work effectively, it is essential that the appropriate management structures exist to support and drive the culture of IG within an organisation. Responsibility for IG should be formally assigned to specified individuals and all staff members should be adequately informed and trained of their own responsibilities in respect of it[10].

Since it would be difficult to describe each of the IG management arrangements for all the health and social care setting in Ireland, this section details the high level IG management structures in place for a number of key organisations such as the Health Service Executive (HSE), GP settings and national data collection sources.

3.1 The Health Service Executive

The Health Service Executive (HSE) is responsible for providing health and personal social services for everyone living in the Republic of Ireland.
The HSE provides numerous different services in hospitals and communities across the country. These services include the treatment of older people in the community, caring for children with challenging behaviour, providing information and support to carers, performing highly-complex brain surgery and controlling the spread of infectious diseases. As result of these transactions, personal health data is collected and processed by services within the HSE.

Ultimately every employee of the HSE has a responsibility to comply with polices and procedures that relate to information governance. As IG covers a variety of topics, the responsibility and management of different aspects of IG falls under different areas. For example the HSE Consumer Affairs Corporate Office is responsible for data protection, and freedom of information requests, while the Information and Communications Technology (ICT) Directorate, in conjunction with relevant data owners, are responsible for the security aspects of electronically held personal health information. In order to bring a more cohesive approach to IG the HSE have set up an Information Governance Framework Project Board and an Information Governance Project Team. However, responsibilities for IG are changing as the HSE structure changes.

The following sections describe how IG is currently managed within the HSE and what initiatives are in place to bring a more cohesive approach.

3.1.1 Information Governance Management in the HSE

IG in the HSE is managed by more than one directorate. Information security assurance for electronically held information is the responsibility of the Information and Communications Technology (ICT) Directorate in conjunction with the relevant data owners. The Consumer Affairs Office of the HSE has been responsible for data protection, freedom of information, and records management assurance since 2005. Specific parts of Records Management, for example in relation to financial records, and the 'hospital chart' have been handled under the aegis of specific operational directorates. At the time of writing this document, these responsibilities in relation to IG are in the process of changing in the context of the HSE internal re-structuring.

3.1.2 Information Security Assurance

The ICT Directorate of the HSE is responsible for voice, video and data communications technologies. The ICT Directorate has a key role, in conjunction with all areas in the HSE, in implementing safeguards for information security assurance in the HSE. A National Director for ICT was appointed in March of 2009, reporting to the National Director for Commercial and Support Services. The National Director is supported at a national level by Directors of Information Systems, the majority of whom have special national lead roles. The ICT Directorate is in the process of developing an ICT Strategy in order to take a coordinated approach to developing ICT in the HSE. In addition to this, and relating specifically to IG, the ICT Directorate has developed a number of HSE policy documents in the area of electronic information security, in consultation with representatives from all of the HSE Directorates. These information security policy documents have been approved by unions and the management team within the HSE. These policies include:

- HSE Information Security Policy
- HSE Electronic Communications Policy
- HSE Encryption Policy
- HSE Password Standards Policy
- HSE Mobile Phone Device Policy

The HSE ICT Directorate will lead on the development of a number of national HSE electronic information security policies in 2010

3.1.3 Data Protection and Freedom of Information Assurance

The Consumer Affairs Office in the HSE is responsible for developing best practice models of customer care, including a statutory complaints handling system, implementing the FOI and Data Protection Acts, and a statutory appeals system.

Within the Consumer Affairs Office there has been a National Lead for freedom of information, data protection and records management. These are three of the core IG topics.

The Consumer Affairs Office is managed by the Head of Consumer Affairs, who has reported through an intervening national director or interim senior manager, to the CEO. The Head of Consumer Affairs is supported by a General Manager for Consumer Affairs in each of the HSE areas.

The General Managers for Consumer Affairs are supported locally by Consumer Affairs Area Officers. At the time of writing of this document the number of Consumer Affairs Area Officers in place in each HSE area varies from one to three.

Each General Manager's Office has overall responsibility for consumer affairs in the particular HSE area and incorporates the following:

- appeals
- complaints handling
- consumer participation
- data protection requests
- freedom of information requests
- ombudsman requests
- ombudsman for children requests
- records management.

The three areas relating to IG are data protection, freedom of information and records management.

Requests for information under Data Protection or Freedom of Information legislation are processed by the Consumer Affairs Area Officers for each specific area. *A Practical Guide for Staff* [46] relating to FOI and Data Protection legislation was published by the National FOI/Data Protection Liaison Officers Group in 2004. This group previously had responsibility for FOI and Data Protection under the Health Board system that pre-dated the HSE.

The Offices of the National Director for Primary, Community and Continuing Care and the National Director for Hospitals have been merged into an Integrated Service Directorate (ISD). Four Regional Director of Operations are now responsible for managing all health and social services in the four regions. In 2007, the Healthcare Records Management Steering Committee published a *Code of Practice for Healthcare Records Management*[18]. The code of practice applies to ISD hospitals and hospitals providing services on behalf of the HSE under Section 39 of the Health Act 2004. Details of the code of practice are outlined in section 6.1 of this report.

3.1.4 HSE Initiatives

As the range of topics covered by IG is quite broad, different entities within the HSE have managed specific aspects of it to date.

However in order to have a more cohesive approach to managing IG the HSE, under the Transformation Programme[4], undertook to develop an IG framework. The purpose of the framework is to ensure that the appropriate structures, policies, and practices for the HSE, are in place to:

- maintain the confidentiality, security and quality of all records
- underpin the proper, full and ethical use of records for the benefit of individuals and for the public good.

A HSE Information Governance Framework Project Board was established to oversee the development and implementation of this. Membership of this group includes the different entities of the HSE that have responsibility for IG for example ICT, Consumer Affairs and the Health Intelligence Unit. Membership also includes representation from the Department of Health and Children, and the Authority.

This project is being pursued primarily because the HSE recognises that information must be protected, but be available as needed, to ensure the best outcomes for patients, clients and staff. The secondary reason is to ensure compliance with prevailing legislative requirements, primarily relating to data protection and freedom of information. The HSE Information Governance

[4] The HSE's Transformation Programme 2007-2010 represents the organisation's ambitions for the future. The programme was prepared following consultation among staff during 2006 and reflects the views expressed during a series of meetings and events across the organisation. It also reflects the views gathered from engagements with the HSE. Specifically the purpose of the programme is 'To enable people to live healthier and more fulfilled lives' and provides the HSE with a shared direction and focus to achieve this.

Framework project addresses the following closely related matters as a coherent whole[47]:

- rights of privacy, confidentiality, consent and access to records
- clinical ethics and professional standards/codes of practice
- guidelines and practice on secondary Uses – for example for research and clinical audit
- information security – which includes but is not only a matter of IT security
- records management
- information quality assurance
- deployment of data standards and definitions.

An IG framework project team was formed in April 2009, reporting to the project board. Membership is comprised of senior managers from the HSE with roles in relation to data protection, freedom of information, information security, records management, and quality and risk. Since establishment, the project team has been working through the development of project deliverables under the aegis of the Project Board. The key deliverables include:

- HSE IG Policy and Procedures
- HSE IG Glossary of Terms and Definitions
- HSE Statement to Service Users – How the HSE Handles Your Information.

In the context of HSE internal re-structuring the IG Framework project is under consideration. The project is awaiting senior management approval to produce and implement HSE IG policies in preparation for the HIQA information governance standards.

The HSE also have a Quality and Risk Management Standard. The aim of this standard is to effectively manage quality and risk by implementing an integrated quality and risk management system that ensures continuous improvement in the quality of the service being delivered[48]. The standard is to be used as part of the implementation of an integrated quality and risk management framework across the HSE.

There are three levels against which compliance with this standard will be assessed. In order to comply with the standard, it is necessary to comply with each of the 22 criteria that have been identified. The aim of the standard is to provide a common set of requirements that will apply across all service providers to ensure that health, personal and social services are both safe and of an acceptable quality. A strategy has been devised to implement the standard in all services managed or funded by the HSE.

A framework for this has been developed by HSE staff in the Integrated Services Directorate. The framework forms a basis for a self- assessment by service providers of the extent to which an integrated quality, safety and risk management system is in place that conforms to the framework and meets the requirements of the overarching HSE Quality and Risk Standard. Within the framework document, the management of patient information is identified as a known high priority risk.

It had been envisaged that standards developed as part of the HSE Information Governance Framework Project might form part of, or be related to the Quality and Risk Management Standard.

3.2 The primary care setting

Within the primary care setting there is no central point of coordination for IG management. The GP is ultimately responsible for all aspects of IG. The Irish College of General Practitioners (ICGP)[5] and the National General Practice Information Technology (GPIT) Group have developed a number of documents that provide guidance in this area. The most notable of these is Managing and Protecting the Privacy of Personal Health Information in Irish General Practice[(49)]. The GPIT Group provides support to GPs in relation to how IG should be managed.

3.2.1 The National General Practice Information Technology (GPIT) Group

The National GPIT Group is a collaborative group comprised of the HSE and the ICGP. There are two parts to the GPIT Group, an educational section with ten GPIT facilitators around the country, and a projects section.

The GPIT facilitators provide support, training and advice to GPs with ICT issues in the different HSE areas. The focus of the GPIT training programme is on practice-based support. Each facilitator focuses on a small number of practices helping them to develop the role of information technology in their practices.

[5] The Irish College of General Practitioners (ICGP) is the professional body for general practice in Ireland. It is the representative organisation on education, training and standards in general practice. The college is the recognised body for the accreditation of specialist training in general practice in Ireland and is recognised by the Medical Council and the Postgraduate Medical and Dental Board as the representative academic body for the specialty of general practice.

In addition to this one-to-one support, there is a "Frequently Asked Questions" section on the GPIT website specifically relating to IT issues in the practice which GPs can access for guidance and advice. This section deals with issues such as sharing of health records, data breaches in the practice and audit trails in GP practices.

3.3 National data sources

Within the Irish health and social care system there are a number of national data sources, which collect data on service-users transacting with the HSE but have independent structures and operate outside the HSE. At the time of writing this report the Authority is undertaking to compile a national inventory of all of the health and social care information sources in Ireland. A selected number of these secondary sources of information are included in this document:

- The National Cancer Registry
- The Health Research Board information systems
- The Economic and Social Research Institute – Hospital In-Patient Enquiry

The independent structure of these bodies has led to independent structures and procedures for IG and IG management.

3.3.1 The National Cancer Registry, Ireland

Established and funded by the Department of Health and Children, the National Cancer Registry (NCRI) was set up in 1991 to record information on all cancer cases and cancer deaths occurring in the Republic of Ireland.

Information is actively gathered by Tumour Registration Officers that are based in hospitals throughout the country. Each is responsible for gathering data from a group of hospitals, and from other sources within a designated geographical area. Within their catchment areas, Tumour Registration Officers liaise with hospital pathology and haematology laboratories, special clinics, hospital administrators and medical records staff. They also maintain links with public health nurses, hospices and nursing homes in the community. The Tumour Registration Officers enter this data onto laptop computers and send it electronically to the NCRI headquarters in Cork where it undergoes quality assurance. Cases are also identified through the death certification system from the Central Statistics Office (CSO).

The NCRI collects identifiable information and the rationale for this are clearly outlined in the document *Data Confidentiality in the National Cancer Registry*[28] which include:

- information on a single cancer often comes from a variety of sources. This duplication of information would inevitably lead to multiple registrations of the tumour, and a gross over-estimation of the incidence of cancer, unless some method were available for linking all information on the same individual
- the NCRI can carry out assessments of the success and coverage rate of screening programmes only if individuals screened can later be identified if they develop cancer
- information on outcome, and particularly survival, is essential to the operation of the registry, and links between registrations and death certificates can only be achieved through the use of some type of personal identification.

Within the NCRI, all staff have responsibility for preserving confidentiality; however, ultimate responsibility rests with the Director of the NCRI, who may ask the Board of the NCRI for guidance in cases which do not conform to the agreed guidelines. The NCRI is subject to both the FOI and Data Protection Acts. Under the FOI Act each person has the right to apply for access to data held by the NCRI. Detailed information on how to apply for access is available to the public on the NCRI website (www.ncri.ie).

The principles of confidentiality can be reconciled with the functions of the NCRI by the adoption of a comprehensive code of practice governing the acquisition, processing, storage and release of identifiable patient data. Where doubt exists as to the appropriateness of a particular line of action, this code of practice must have as its highest priority the protection of the rights of the individual patient.

The NCRI currently makes a large volume of information available to the public in relation to its functions and activities. The NCRI imposes a number of conditions on the release of data and all data requests are approved by the Director.

The operation of the NCRI itself is largely electronic. Data within the NCRI is protected by passwords and encrypting and data collected by NCRI staff on laptop computers is password protected and encrypted, and is also encoded during any transmission to the NCRI via modem[28].

All staff concerned with the collection, processing and output of personal data are employees of the NCRI. On commencing work they are asked to:

- read, agree to and observe the rules set out in *Guidelines for staff on confidentiality within the National Cancer Registry*[28]
- to sign an undertaking of confidentiality, which will remain binding even following their departure from Registry work. This undertaking prohibits staff from disclosing, wither directly or indirectly, to any individual outside the Registry, the identity of any person registered, or any data concerning such an individual, or any other confidential material they may come across in the course of their work
- to observe the security precautions in operation within the Registry.

3.3.2 The Health Research Board

Within the Health Research Board (HRB) the Health Information Directorate manages all the HRB's national health information systems. The directorate comprises three specialist units that have responsibility for national databases, as depicted in table 1.

Table 1 – HRB specialist units and corresponding databases

HRB Specialist Unit	National Databases
Alcohol and Drug Research Unit	National Drug Treatment Reporting System National Drug-Related Deaths Index
Disability Databases Unit	National Intellectual Disability Database National Physical and Sensory Disability Database
Mental Health Research Unit	National Psychiatric In-Patient Reporting System (NPIRS)

Within the HRB, policies and procedures have been developed individually for each of the information systems – including those relating to security and other IG topics. The following section details the work of the Disability Database Unit making reference to the National Intellectual Disability Database (NIDD).

The Disability Databases Unit manages two national service-planning databases for people with disabilities on behalf of the Department of Health and Children. These disability databases aim to provide a comprehensive and accurate information base for decision-making in relation to the planning of specialised

health and personal social services for people with intellectual, physical or sensory disabilities. The NIDD collects information on those with an intellectual disability and was established in 1995. The NIDD is a set of information that outlines the specialised health services currently used or needed by people with intellectual disability. The database informs the regional and national planning of these services by providing information on trends in demographics, current service use and future service need[28]. The NIDD is governed by the National Intellectual Disability Database Committee which has representation from the Department of Health and Children, the HSE, the National Federation of Voluntary Bodies and the HRB.

The NIDD is a web-enabled centralised system through which HSE areas and service providers can enter, access, and update relevant information. The HSE is responsible for the implementation and maintenance of structures for the identification of individuals and the collection, review and updating of data. The initial step in the generation of the national dataset is the completion of a data form for each identified individual. The HRB develops and maintains software to facilitate the collection and reporting of NIDD data[50]. The first step in the collection of this information is the completion of a database form for each individual who meet the registration criteria. Before the form is completed, the consent of the individual and/or his/her next of kin is sought. The information is gathered by both statutory agencies (the HSE) and non-statutory service-providers. Dedicated personnel within the HSE Local Health Offices enter or upload the data from these forms to a web-based database called the National Intellectual Disability Database.

The NIDD collects four types of information as follows:

- personal and demographic details
- residential, day, and support services that are currently received
- residential, day and support services that are required in the next five years
- additional information to assist with the administration of the database.

Access to the data held on the NIDD is set out in a protocol agreed by the national committee. Levels of access vary from full access to national anonymised data (HRB, Department of Health and Children) to regional and local access by HSE personnel depending on level of responsibility and access by service provider agencies to the data on their own service users. This protocol also sets out data security guidelines for the NIDD. Access to the data held is password protected so that only authorised users can access the system.

The HRB designs and delivers a standardised training programme for both data collection and for software and provides frontline support to NIDD software

users. The HRB updates the manual for the NIDD each year. This manual sets out the guidelines for use of the database, the areas of responsibility that are assigned to each organisation and the coding and programme details covered. The manual is available to download from the system. At the time of writing this report the database has 26,023 registrations and is being used in all HSE areas and by approximately 120 service providers[51].

In relation to IG the previously mentioned NIDD Committee has responsibility for the database. The composition of the committee is designed to reflect the key stakeholders involved. Requests for information from the national dataset are made to this committee. The committee authorises or refuses requests for information on the basis of the appropriateness of the request. Decisions are made based on consensus and a process of negotiation is often entered into to clarify the request or to seek reassurance regarding the methodology of the study or the proposed use of the data[52]. It is noteworthy that the NIDD does not hold identifiable data about individuals. Each individual is assigned a Personal Identification Number. Under data protection legislation every effort is made to preserve the confidentiality of the individual. In addition, the NIDD acknowledges the rights of individuals or their families to access the information held under the legislative provisions of the Data Protection and Freedom of Information Acts[50].

3.3.3 The Economic and Social Research Institute - HIPE

The Economic and Social Research Institute (ESRI) produces research that contributes to understanding economic and social change and that informs public policy making and civil society in Ireland and throughout the European Union. The Health Research and Information Division (HRID) of the ESRI is responsible for two databases of national data

- the Hospital In-Patient Enquiry (HIPE) system
- the National Perinatal Reporting System (NPRS).

HIPE is the principal source of national data on discharges from acute hospitals in Ireland. NPRS provides national statistics on perinatal events, in particular data on pregnancy outcomes, perinatal mortality and other important aspects of perinatal care. HIPE and NPRS are administered by the ESRI under contract from the HSE.

HIPE data are managed on a distributed database (W-HIPE), developed and supported by HRID. Each participating hospital runs a local version; anonymised data are collated to a national file in the ESRI on a monthly basis. Confidentiality of patient and consultant information is maintained at the national level, by not

incorporating patient name and encrypting consultant information. Access to W-HIPE is controlled and password protected. All changes made at the local level are audited; data cannot be changed at the national level. Encryption is applied to all data transfers.

Administrative and demographic information is downloaded from hospital patient administration systems directly. Coders verify this information and extract clinical information on diagnoses and procedures from hospital patient records. HRID provides training support on coding methodology; including the extraction from records and the classification of information. Irish Coding Standards are published to supplement the international classification system. Detailed checks run at the point of entry to minimise data errors, supplemented by data quality activities at the national level, to ensure consistency across hospitals. Audits are conducted at local and national level to check the accuracy of HIPE information. Ongoing data quality review is an important function of the entire HIPE process.

Aggregate national statistics, without identification of patient, hospital, or consultant are available through a number of channels;

- data is reported annually in the Activity in Acute Public Hospitals Ireland report series
- the Online Data Reporter (www.esri.ie/health_information/hipe_data_reporter/) allows access to aggregated HIPE data and perform analyses. In order to gain access to this reporter the user must accept the terms and conditions
- individual requests for HIPE data must be accompanied with a completed HIPE Data request form, available online. On receipt of data, users must agree to the conditions of use of HIPE data
- datasets are made available on request; variables are excluded to prevent identification of patient, hospital and consultant. Datasets are encrypted and password protected.

When reporting the ESRI does not disclose cells where the number of discharges reported to HIPE is five or less. Such cells are replaced by "~". Where further suppression is necessary to ensure that cells with five or less discharges are not disclosed, it may be necessary to suppress the cell with the next lowest number of discharges. These cells have been replaced with "*". Finally, where necessary to ensure additional confidentiality, selected rows are aggregated.

3.4 Summary

In order for IG to work to the full effect, derive the benefits associated with it and protect the interests of patients and service-users, it is essential that the

appropriate management structures are in place to support it. Different management structures, processes and procedures have emerged in relation to the management of information in the organisations studied, in part due to different governing structures and the type of information collected. Significant developments have taken place within each in the form of structures, guidance and processes that have been put in place in respect of IG. What has been developed and put in place varies significantly across but also within organisations, for example in the HRB, where each individual unit has developed policies and procedures, which highlights the absence of and reinforces the need for a single coordinated point of reference and guidance for IG.

4 Confidentiality and data protection assurance

Confidentiality and data protection assurance is driven by the Data Protection Acts of 1988 and 2003[11;12]. The Data Protection Acts apply to both public and private health and social care organisations. Confidentiality refers to a duty that a person owes to safeguard information that has been entrusted to him or her by another. In the healthcare context, care providers have confidentiality duties in regard to their patients that are founded on and emphasised by both longstanding ethical duties and legal principles[2].

Confidentiality and data protection are important to ensure compliance with the legislation and to promote patient-centred care. Organisations must be compliant with the Data Protection Acts of 1988 and 2003[11;12] , and therefore, require processes to ensure that all processing of personal information is carried out confidentially. Organisations should ensure that patients and service-users are adequately made aware of their choices as regards the sharing of their information.

A number of guidelines have been produced in respect of this aspect of IG. Some are general and apply to all the public sectors such as *Guidelines on Protecting the Confidentiality of Personal Data* [53], and some are specific to health such as *A Guide to Professional Conduct and Ethics for Registered Medical Practitioners*[43]. The following sections describe the scope of these guidelines. This list is not exhaustive but rather a sample of what currently exists in Ireland.

- *Guidelines on Protecting the Confidentiality of Personal Data*[53]
- *Data Confidentiality in the National Cancer Registry*[28]
- *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice – An Information Guide to the Data Protection Acts for General Practitioners*[49]
- *Interim Guidelines on Information Sharing in Primary Care Teams*[18]
- *Data Protection Acts 1988 and 2003 - A Guide for Data Controllers*[54]
- *A Guide to Professional Conduct and Ethics for Registered Medical Practitioners*[43]
- *The Code of Professional Conduct for each Nurse and Midwife*[40]
- *The Data Protection Acts 1988 and 2003: Some implications for public health and medical research – a discussion document* [55].

4.1 *Guidelines on Protecting the Confidentiality of Personal Data*

These guidelines were published by the Centre for Management and Organisation Development (CMOD), the Department of Finance in 2008 to assist departments, offices and public agencies of the State in implementing systems

and procedures that will ensure, as much as possible, that personal data in their possession is kept safe and secure and to help departments, offices and agencies to meet their legal requirements under the Data Protection Acts[11;12] . Although the document is called a guidance note, its contents are in fact mandatory, and departments, offices and agencies are expected to implement the guidelines with immediate effect. Within the health and social care sector it applies to all public providers of health services, including the HSE.

Title: *Protecting the Confidentiality of Personal Data*[53]

Author: The Centre for Management and Organisation Development (CMOD), the Department of Finance

Date Published: December 2008

Audience: All public bodies

Topics covered: The following topics are covered:

- general procedures
- paper records
- e-mail and personal productivity software
- electronic remote access
- laptops/notebooks
- mobile storage devices
- data transfers
- inappropriate access/audit trail monitoring
- breach management.

URL: http://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf

4.2 *Data Confidentiality in the National Cancer Registry*

The National Cancer Registry, collects, records, stores and analyses information relating to the incidence and prevalence of cancer and related tumours in Ireland. In 2007, the NCRI published guidelines set out the broad principles and practice relating to data confidentiality and security within the NCRI[28]. The guidelines define confidential data as any personal health information relating to an identified or identifiable person. Data presented in statistical form, which can no longer be reasonably identified, are not considered as personal data. Although

the definition of "confidential" information used here is similar to that given for "sensitive personal" data in the Data Protection Acts, the Registry definition is extended to cover deceased persons, who are not covered by the Data Protection Acts[11;12].

The guidelines note that the principles of confidentiality apply, not only within the Registry, but also to any data released by it, whether for public information, or to individual researchers. In particular, the Registry must take care not to publish data, or to provide it for publication by others, in a way that would allow any individual to be indirectly identified.

Title: *Data Confidentiality in the National Cancer Registry*[28]

Author: The National Cancer Registry, Ireland (NCRI)

Date Published: 2007

Audience: NCRI staff and members of the public that wish to request data from the Registry

Topics covered: The following topics are covered:

- principles and practice relating to data confidentiality and security within the NCRI
- procedures for the release of data
- methods of achieving data security and confidentiality of data
- guidelines for staff.

URL: http://www.ncri.ie/data.cgi/html/NCRI-data-confidentiality.rtf

4.3 *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice*

Managing and Protecting the Privacy of Personal Health information is Irish General Practice was published in 2003[49]. Recognising that every practice is different, the document recommends that practices consider preparing an information management and privacy policy document setting out procedures for the management of personal held information obtained and held by the practice. It should also identify the specific responsibilities of practice members individually and the practice collectively.

This document also addresses principles of information management and multidisciplinary primary care teams. Where such teams are established, it is recommended that a nominated person within the team structure should have responsibility for overseeing the implementation and effective operation of the team's policy on managing personal health information. In the context only of the team providing an integrated package of care, certain personal data obtained by different members of the primary care team may need to be shared with other team members. Therefore, it is particularly important that the issue of the sharing of certain personal health information and especially the principle of patient consent to any such sharing, is carefully addressed. Appropriate arrangements should also be in place to govern access by administrative staff in fulfilment of their duties within the team.

The precise content of the practice's information policy document will depend on the organisational and personnel structure of each practice and the record keeping system used. In each case it is recommended that the document include specific provision for staff training and education in relation to data protection law and confidentiality.

Title: *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice*[49]

Author: The ICGP and GPIT Group

Date Published: November 2003

Audience: Primary care teams

Topics covered: The following topics are covered:

- legal and ethical provisions
- principles
- personal health information
- quality, retention and security of personal health information
- using, disclosing and transferring personal health information
- patient consent
- patient access to personal health information
- a practice policy on personal health information.

URL: http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports

4.4 *Interim Guidelines on Information Sharing in Primary Care Teams*

These guidelines were developed by the Information Sharing Framework Working Group in 2008[56]. The aim of the guidelines is to ensure compliance with privacy, confidentiality and security of service-user healthcare information shared by primary care teams, consistent with the duty of care. The purpose of the guidelines is to provide service-users with coordinated and seamless care, and to foster service user confidence. It is thought that this will be achieved by facilitating and supporting all staff in primary care teams (PCTs) in making good decisions about the protection, use and disclosure of service-user information, while taking account of their ethical and legal obligations.

Title: *Interim Guidelines on Information Sharing in Primary Care Teams*[56]

Author: The Information Sharing Framework Working Group – comprised of service users, general practitioner representatives, representatives of the Office of the Data Protection Commissioner and HSE staff representatives

Date Published: 2008

Audience: Primary care team members

Topics covered: The following topics are covered:

- core principles
- duty of care
- referral
- open access to records
- clinical team meetings
- information security
- consent to share service user information
- disclosing information without consent
- client access.

URL: Not available

4.5 *Data Protection Acts 1988 and 2003 - A Guide for Data Controllers*

This guide, published by the Office of the Data Protection Commissioner, is an introductory guide to persons/bodies who are data controllers. It outlines the eight fundamental rules of data protection and the way in which to comply with these rules. The Guide also includes a basic data protection checklist.

Title: *Data Protection Acts 1988 and 2003 – A Guide for Data Controllers*[54]

Author: The Office of the Data Protection Commissioner

Date Published: February 2008

Audience: Those persons/bodies who are data controllers, in that they control the contents and use of personal data

Topics covered: The following topics are covered:

- responsibilities of data controllers
- compliance with the law
- how the Acts are enforced
- the eight rules of data protection
- transferring personal data abroad.

URL: http://www.dataprotection.ie/documents/forms/NewAGuideForDataControllers.pdf

4.6 *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*

The Medical Council updated their guidance for medical practitioners on ethical conduct and behaviour in November 2009[43]. Doctors working in Ireland have a responsibility to ensure compliance of their records systems with current Irish data protection and freedom of information legislation. Section C of the document deals with medical records and confidentiality and is of particular relevance for IG. The section covers the general principles of confidentiality in addition to the disclosure of information, the information that patients receive, registers of illness and the recording of information.

The guidelines were produced to govern the relationship between doctors and patients.

Title: *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*[43]

Author: The Medical Council[6]

Date Published: November 2009 (7th edition)

Audience: Medical professionals

Topics covered: The following topics are covered:

- professional conduct
- responsibilities to patients
- medical records and confidentiality
- consent to medical treatment
- professional practice

URL: http://www.medicalcouncil.ie/_fileupload/misc/171109%20Final%20Version%20Ethics%20Guide%20Update%20For%20Printer.pdf

4.7 *The Code of Professional Conduct for each Nurse and Midwife*

An Bord Altranais[7] published the *Code of Professional Conduct for each Nurse and Midwife* in 2002[40]. Ethical and legal considerations inform professional decision-making related to record management and the sharing of information. Managers of the nursing and midwifery services have a responsibility to ensure that systems are in place to support practitioners in relation to this aspect of their clinical work.

The purpose of this code is to provide a framework to assist nurses in making professional decisions, being able to carry out his/her responsibilities, and to promote high standards of professional conduct. The code states that information regarding a patient's history, treatment, and state of health is privileged and confidential. It is accepted nursing practice that nursing care is

[6] The Medical Council is the statutory regulatory body for the medical profession in Ireland
[7] An Bord Altranais is the statutory body responsible for the registration and education of nurses and midwives, as well as for all matters relating to the practice of nursing and midwifery in Ireland

communicated and recorded as part of the patient's care and treatment. Professional judgement and responsibility should be exercised in the sharing of such information with professional colleagues. The confidentiality of patient records must be safeguarded. In certain circumstances, the nurse may be required by a court of law to divulge information held. A nurse called to give evidence in court should seek legal and/or professional advice in advance as to the response to be made if required by the court to divulge confidential information.

It is necessary for patients to have appropriate information for making an informed judgement. Every effort should be made to ensure that a patient understands the nature and purpose of their care and treatment. In certain circumstances there may be a doubt whether certain information should be given to a patient and special care should be taken in such cases.

Title: *The Code of Professional Conduct for each Nurse and Midwife*[40]

Author: An Bord Altranais

Date Published: November 2002

Audience: Nurses and midwives

Topics covered: The following topics are covered:

- professional behaviour
- sharing of information
- principles of confidentiality
- use of personal health information in research.

URL: http://www.lenus.ie/hse/handle/10147/44988

4.8 *The Data Protection Acts 1988 and 2003: Some implications for public health and medical research – a discussion document*

This discussion document examines some of the legal and practice ramifications of the Data Protection Acts 1988 and 2003[11;12] for public health and medical research. The paper was commissioned by the HRB subsequent to the expression of general concerns in relation to how the legislation applies to public health and medical research.

Title: *The Data Protection Acts 1988 and 2003: Some implications for public health and medical research – a discussion document*[55]

Author: Asim Sheikh, commissioned by the HRB

Date Published: July 2008

Audience: Bodies with an interest in public health and medical research

Topics covered: The following topics are covered:

- legal issues around privacy and confidentiality relating to medical information
- the Data Protection Acts – in general and with specific regard to medical research
- disclosure of records of the deceased
- overview and selected comparison with other jurisdictions.

URL: http://www.hrb.ie/research-strategy-funding/publications/rsf-publication/publications//411/

4.9 Summary

The documents and guidelines discussed under confidentiality and data protection assurance are primarily driven by the Data Protection Acts[11;12] and the common law duty of confidentiality. Some are not sector-specific, while others focus on providing general guidance in relation to legislative requirements and best practice in managing information in such a way that protects the rights of patients and service-users.

5 Information security assurance

Information security assurance requires organisations to have systems that ensure information assets of all types are held confidentially, can be relied upon in use, and are available to authorised persons when and where needed[10]. It is concerned not only with technical methods for securing information but also with physical security measures. Security is important to prevent security breaches and to protect the confidentiality and privacy of information. Patients need to be assured that their personal information is secure – whether it is in manual or electronic form.

The following is a sample of what has been developed in respect of information security; it is not intended to be an exhaustive list of the work that has been done in this area but rather examples of good practice:

- *No Data, No Business: Information Communication Technology (ICT) Security Guidelines*[57]
- *Data Protection Guidelines for Developing Security Policies*[58]
- *Data Confidentiality in the National Cancer Registry*[28]

The ICT unit in the HSE has also undertaken the development of a number of guidelines and policy documents relating to information security that are at various stages of development (as detailed in section 3.1.1 of this document). This forms part of a wider programme of work around IG. The ICT unit in the HSE is only responsible, in conjunction with the relevant data owners, for the security of electronic records including physical access to the areas like server rooms but is not responsible for the physical paper records.

5.1 *No Data, No Business: Information Communication Technology (ICT) Security Guidelines*

These guidelines were developed by the General Practitioners Information Group (GPIT) in 2008[57]. Many practices now have a software system in place to manage patient information and the day-to-day operation of the practice has become reliant on its operation. General practices hold confidential patient information which must be protected. To help practices deal with ICT security, a checklist has been developed which highlights key areas that should be addressed to prevent computer systems from being compromised. In addition to the checklist, security guidelines have been developed which give more detail on the key aspects of ICT security which need to be addressed and implemented.

Title: *No Data, No Business: Information Communication Technology (ICT) Security Guidelines*[57]

Author: The GPIT Group

Date Published: January 2008

Audience: General practitioners and primary care teams

Topics covered: The following topics are covered:

- policies and procedures
- firewall
- malware
- physical security
- access control
- laptop use
- wireless
- back up guidelines
- ICT security checklist.

URL: http://www.icgp.ie/go/in_the_practice/information_technology/news_updates/E3E7417C-19B9-E185-833C5534D98B3B8C.html

5.2 *Data Protection Guidelines for Developing Security Policies*

The Office of the Data Protection Commissioner published these guidelines in 2008[58]. The Data Protection Acts do not detail specific security measures that a data controller or data processor must have in place. Rather, Section 2(1) (d) places an obligation on persons to have appropriate measures in place to prevent "unauthorised" access to, or alteration, destruction or disclosure of, the data and against their accidental loss or destruction. The amended Act in 2003 clarified the nature of security measures required to demonstrate compliance with Section 2(1) (d). When determining security measures, a number of factors need to be taken into account:

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

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

Title: *Data Protection Guidelines for Developing Security Policies*[58]

Author: The Office of the Data Protection Commissioner

Date Published: December 2008

Audience: Data processors and controllers

Topics covered: The following topics are covered:

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

URL: http://dataprotection.ie/viewdoc.asp?m=&fn=/documents/responsibilities/sg160204.htm

5.3 *Data Confidentiality in the National Cancer Registry* (as detailed in Section 4.2) – *Appendix 4: Procedures for data security*

Appendix 4 of Data Confidentiality in the National Cancer Registry sets out the requirements of staff in relation to confidentiality and security precautions in the Cancer Registry.

Title: *Data Confidentiality in the National Cancer Registry*[28] within the Registry

Author: The NCRI

Date Published: 2007

Audience: NCRI staff

Topics covered: The following topics are covered:

- staff
- physical security
- electronic security.

URL: http://www.ncri.ie/data.cgi/html/NCRI-data-confidentiality.rtf

5.4 Summary

Information security has come more to the fore recently as a key issue in IG, primarily due to the shift toward electronic records and systems. As a result much of the focus has been on ICT systems and technical issues, however physical security measures warrant equal consideration. Information is an important resource in delivering safe and effective health and social care services and as such ensuring that it is secure is of great importance. Informed primarily by the requirements of different care settings, organisations have developed their own security policies. The HSE ICT unit is currently developing national guidelines and policies in this area.

6 Clinical information assurance / care records assurance

Clinical information assurance/care-records assurance is concerned with ensuring clinical/care records are of high quality. High quality information is information that is accurate, reliable and up-to-date so that service providers can be confident with their care decisions. Clinical information assurance also requires that organisations implement measures to ensure the availability of clinical/care records when and where they are required[10].

It relates to the quality of the information that is collected and impacts on patient safety as the information available is the basis for clinical decision-making. It also relates to the way in which information is recorded and stored, which impacts on efficient service delivery.

A number of policies, documents and guidelines have been produced in respect of this aspect of IG. This is a sample from this list:

- *The Healthcare Records Management Code of Practice*[18]
- *Records Management Handbook*[59]
- *Recording Clinical Practice Guidance to Nurses and Midwives*[60]

6.1 *The Healthcare Records Management Code of Practice*

The *Healthcare Records Management Code of Practice* was published by the National Hospitals Office in 2007[18]. The code outlines a framework for best practice in ensuring consistent, coherent healthcare records management in all public and private healthcare facilities throughout the country. The document applies to all patient information collected including electronic and paper based records, photographs, slides, x-rays and birth/operation certificates.

Title: *The Healthcare Records Management Code of Practice*[18]

Author: The National Hospital's Office (NHO)[8]

Date Published: October 2007

Audience: NHO hospitals and hospitals providing services on behalf of the

[8] With the establishment of the NHO, acute hospital services are now managed on a single national basis. The NHO is responsible for the strategic management of acute hospital services for the country.

Health Service Executive under S.39 of the Health Act 2004

Topics covered: The following topics are covered:

- standards
- recommended practices for clinical staff
- recommended practices for healthcare records staff
- retention and disposal schedule
- audit tool.

URL: http://213.94.192.205/en/Publications/HSEPublicationsNew/AcuteHospitalReportsGuidelines/NHOCodeofPracticeonHealthcareRecords/FiletoUpload,6884,en.pdf

6.2 *Records Management Handbook*

In November 2004 the Office of the Information Commissioner (OIC) published its *Records Management Handbook*[59]. The handbook includes policies for records management and detailed guidelines and procedures for the handling of OIC documents and other forms of records. It also sets out the retention and destruction policies for such records. The handbook provides guidance to OIC staff on the management of records and it is hoped that the model for records will prove useful to other public bodies developing or refining their own record management policy and practice.

Title: *Records Management Handbook*[59]

Author: The Office of the Information Commissioner

Date Published: November 2004

Audience: Staff of the Office of the Information Commissioner and all public bodies

Topics covered: The following topics are covered:

- records management – the context
- records management standards
- records management policies
- records management procedures
- governance mechanisms.

URL: http://www.oic.gov.ie/en/Publications/OfficeManuals/RecordsManagementHandbook/

6.3 *Recording Clinical Practice Guidance to Nurses and Midwives*

Recording Clinical Practice Guidance to Nurses and Midwives was published in 2002 by An Bord Altranais[60]. The aim of this document is to assist nurses and midwives:

- to appreciate the professional and legal issues regarding the compilation and management of nursing and midwifery documentation
- to value professional responsibility associated with good practice in records management
- to offer practical advice in attaining/maintaining acceptable standards of recording clinical practice.

Among the specifically identified indicators of competence for nurses and midwives is one that stipulates that an individual nurse should "establish and maintain accurate, clear and current client records within a legal and ethical framework". This requirement is irrespective of whether the records are hand-written or electronic.

The section of the document outlining the guidelines for good practice in recording clinical practice outlines 19 guidelines including the following:

- all narrative notes are individualised, accurate, up to date, factual and unambiguous
- all entries are signed and dated
- all written data in respect of a patient/client/family should be kept in a designated area with a view to forming a complete single record
- regular audit is an integral part of maintaining quality records.

Title: *Recording Clinical Practice Guidance to Nurses and Midwives*[60]

Author: An Bord Altranais

Date Published: November 2002

Audience: Nurses and midwives

Topics The following topics are covered:

covered:

- purposes of good records management
- confidentiality
- documenting consent to treatment
- legal considerations
- use of records in research
- guidelines for good practice in recording clinical practice.

URL: http://www.lenus.ie/hse/handle/10147/45061

6.4 Summary

Clinical information assurance relates to the quality of information that is collected. The information available at a point of care determines the care that is received thereby impacting on patient safety and potentially increasing the efficiency of services provided. A key aspect impacting on data quality is the training of staff collecting the information. In relation to IG the main issue is records management as this ensures that the information is available when and where it is needed and also allows for uniformity in the way information is recorded. A number of policies, documents and guidelines have been produced in respect of this topic. The guidelines, both generic and health and social care specific, apply to all types of records whether paper or electronic and with specific regard to healthcare also include x-rays and slides.

7 Secondary use assurance

The secondary use of information relates to information being used for reasons other than direct patient-care that is, for purposes which will not have a direct benefit for the patient concerned. For example, information may be used for research purposes or for clinical audits. Guidelines in this area assure patients and service-users that their data is not being used inappropriately and that any personally identifiable information is not being used without their consent. Such guidelines enable compliance with the data protection legislation in relation to this area. The secondary use of information is important for clinical audits, to conduct research and to inform service delivery, but in using it for these purposes organisations must ensure that the rights of the patients are protected.

Secondary sources of information include the NCRI, HIPE data collected by the ESRI and the databases operated by the HRB.

A number of policies, documents and guidelines have been published in respect of this aspect of IG. The following is a sample of such documents:

- *Data Protection Guidelines on Research in the Health Sector*[19]
- *Guidance to Nurses and Midwives Regarding Ethical conduct of Nursing and Midwifery Research*[41]
- *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice. Appendix 2 – Use of Personal Health Information for Medical Research Purposes, Quality Assurance and continuing Professional Development and Teaching Purposes*[49].

7.1 *Data Protection Guidelines on Research in the Health Sector*

The *Data Protection Guidelines on Research in the Health Sector* were published by the Office of the Data Protection Commissioner in 2007[19]. These guidelines concentrate on the gathering of patient data for a research and clinical audit purposes. The subsequent conduct of research or clinical audit project would also need to comply with data protection legislation particularly in relation to access to and the safekeeping of the data. The guidelines aim to strike a balance between the patient's right to personal data privacy and the desirability of making data available for research. The document strives to present a position whereby the principles of data protection can promote and work with research and clinical audit once the patient's basic right to privacy is respected.

At its simplest, the requirements can be reduced to an obligation to respect the confidentiality of information about patients. Under the Data Protection Acts, the

responsibility for ensuring the confidentiality of patient data and for securing any necessary consent for its further use lies with the data controller. It is this data controller who is legally responsible for the processing of the data under the Data Protection Acts. The most straightforward way in which access to patient identifiable information for research or clinical audit purposes can take place in line with the requirements of the Acts, is with the consent of the person for the intended use.

Anonymisation or pseudonymisation[9] (subject to adequate safeguards) should be explored as the optimal position in relation to patient identifiable information where it might be used for research or clinical audit purposes and adopted if at all possible. This is the ideal solution in cases where capturing consent is deemed particularly difficult.

Clinical audit is in some cases different from research in that it normally takes place within a hospital and has the potential to be of direct benefit to a patient who is in receipt of regular treatment and whose treatment is reviewed by a clinical audit team. In situations where direct benefit to a patient can be clearly demonstrated or where all access to patient identifiable data will take place for the purposes of audit by staff members of the health facility, it may be considered sufficient to rely upon the provisions of the Acts where the processing is necessary for 'medical purposes' and carried out by a health professional or a person "who in the circumstances owes a duty of confidentiality to the data subject that is equivalent to that which would exist if that person were a health professional".

These guidelines recommend that as much information as possible be provided to patients in a patient information leaflet. It is recommended that these leaflets outline how data may be disclosed in the future for the benefit of the patient, or for purposes not directly related to, or indeed completely separate from, the patient's own healthcare treatment.

Title: *Data Protection Guidelines on Research in the Health Sector*[19]

Author: The Office of the Data Protection Commissioner

Date Published: November 2007

[9] Pseudonymisation involves the use of a coding system to protect the identify of an individual to whom the information relates. Pseudonymous records are distinguishable but cannot be associated with a specific person. It eliminates the need to retain all identifying characteristics with the data.

Audience: Data controllers

Topics covered: The following topics are covered:

- the data protection background
- the use of patient information for research purposes
- clinical audit.

URL: http://www.dataprotection.ie/documents/guidance/Health_research.pdf

7.2 *Guidance to Nurses and Midwives Regarding Ethical Conduct of Nursing and Midwifery Research*

These guidelines were published in 2007 by An Bord Altranais and state that when patient/client records are utilised in research, they are subject to the same ethical considerations as any other type of research. The principles of privacy, confidentiality and anonymity must be respected. Competence in research requires that confidentiality be ensured in respect of records. In addition, the researcher must:

- adhere to the institutional policy regarding records
- abide by the Data Protection Acts, 1988 and 2003
- consider the rights of patients/clients, past and present, whose records are to be utilised in research and which may involve seeking their written consent.

Title: *Guidance to Nurses and Midwives Regarding Ethical Conduct of Nursing and Midwifery Research*[41]

Author: An Bord Altranais

Date Published: January 2007

Audience: Nurses and midwives

Topics covered: The following topics are covered:

- ethical principles
- considerations when undertaking research
- ethical conduct and the research process

- use of records in research
- clinical trials.

URL: http://www.nursingboard.ie/GetAttachment.aspx?id=322b92ac-60f6-48c6-8ec6-88c087a8013f

7.3 *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice*

Appendix 2 of the document notes that as a general rule, personal health information can only be used for the purpose of medical research with the written consent of the patient who has an understanding of what the proposed research entails and the ways in which the personal health information will be used.

In a small number of cases, it may be possible to dispense with the need for written consent, such as where the research is to be carried out by the treating GP without any third party access to the personal health information. Even in this case, however, patients should be made aware that their personal health information could be used in this way so that they have an opportunity to withhold their information from the research project if they so choose. This also applies when a practice is carrying out research using anonymised data. However, care needs to be taken to ensure that no patient can be identified especially in the case of small groups of patients with unusual conditions.

In all other cases, patient consent should be given and research must be approved by an appropriate body. Where the records of a practice are used for carrying out public health or other medical research using anonymised data, patients of the practice should be made aware of this use of their records.

All research records should be anonymised at the earliest possible time in line with the proper conduct of the research.

In relation to quality assurance and continuing professional development activities, the document states that personal health information can be used where:

- the activities are directly related to the purpose for which the information was collected and are within the reasonable expectations of the patient
- the patient has given express consent for the use of personal health information for these activities
- the personal health information has been anonymised

- the activities involve research or the compilation of statistics, have been approved by a properly constituted Human Research Ethics committee, and are conducted in accordance with that committee's requirements and data protection law.

Wherever possible, personal health information should be anonymised before it is used for teaching purposes. Where this is not possible, the doctor should be certain that the patient understands and agrees to this use.

Title: *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice*. (As detailed in section 4.5) *Appendix 2: Use of Personal Health Information for Medical Research Purposes, Quality Assurance and Continuing Professional Development and Teaching Purposes*[49]

Author: The ICGP and GPIT Group

Date Published: November 2003

Audience: General practitioners and primary care teams

Topics covered: The following topics are covered:
The use of personal health information for:
- medical research
- quality assurance
- continuing professional development
- teaching purposes.

URL: http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports

7.4 Summary

The secondary use of information can yield significant developments and improvements in service delivery, for example through clinical audit and the use of information in research. However in order for this to continue and for patients and service users to be comfortable with the use of their information they need to be confident that their rights, and their identity in many cases, are being appropriately protected and respected.

Recognising this need, a number of policies and guidance documents have been developed. These are primarily based on the provisions in the Data Protection Acts[11;12], and it is likely that these will be further refined and expanded by provisions in the forthcoming Health Information Bill.

8 Freedom of information assurance

Freedom of information assurance is driven by the requirements of the Freedom of Information Acts 1997 and 2003[13;14]. The work area requires that organisations implement measures to ensure compliance within the limited timescales for responding to an information access request. It also requires an appropriate records management strategy and an accountable staff member.

The following are a sample of guidance document in respect of this aspect of IG:

- *Short Guide to the Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003*[23]
- *Manual for Freedom of Information Decision Makers*[61]
- *Freedom of information Acts 1997 and 2003, Data Protection Acts 1988 and 2003, Administrative Access Policy – A Practical Guide for Staff*[46]

8.1 *Short Guide to the Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003*

This guide, developed by the Department of Finance in 2003, provides detailed information on the provisions contained in the Freedom of Information Acts and what is expected of public bodies in order to be compliant with them [23].

Title: *Short Guide of the Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003*[23]

Author: FOI Central Policy Unit, the Department of Finance

Date Published: July 2004

Audience: All public bodies, including the HSE and voluntary hospitals

Topics covered: The following topics are covered:

- introduction
- public requirements
- processing requests
- exemptions
- restrictions of the Acts
- review of decision
- charges
- training and further information.

URL: http://www.foi.gov.ie/short-guide-to-the-foi-acts

8.2 *Manual for Freedom of Information Decision Makers*

The purpose of this manual, developed by the Department of Finance is to advise decision makers when processing freedom of information requests[61]. A section is included detailing the exemptions that apply under the Act and the rights inferred on individuals by it.

Title: *Manual for Freedom of Information Decision Makers*[61]

Author: The FOI Central Policy Unit, the Department of Finance

Date Published: October 2004

Audience: All public bodies, including the HSE and voluntary hospitals

Topics covered: The following topics are covered:

- processing FOI requests
- exemptions and consultation procedures
- common policy issues
- right to amend personal information
- right to reasons for decisions
- Information Commissioner decisions

URL: http://www.foi.gov.ie/decision-makers-manual

8.3 *Freedom of Information Acts 1997 and 2003, Data Protection Acts 1988 and 2003, Administrative Access Policy – A Practical Guide for Staff*

This document was developed by the National FOI/DP Liaison Officers Group under the health board system that preceded the HSE[46]. The guide is designed to explain the main provisions of data protection and FOI legislation. There is also a section detailing administrative access, that is, how to obtain personal information in a routine and informal way.

Title: *Freedom of information Acts 1997 and 2003, Data Protection Acts 1988 and 2003, Administrative Access Policy - A Practical Guide for Staff*[46]

Author: The National FOI/DP Liaison Officers Group, formerly of the Health Boards, now the HSE

Date Published: 2004

Audience: Health board staff/ HSE staff

Topics covered: The following topics are covered:

- Freedom of Information Acts 1997 and 2003
- Data Protection Acts 1988 and 2003
- Administrative Access Policy
- responsibilities for staff

URL: Not available

8.4 Summary

Freedom of information assurance is driven by the provisions of the Freedom of Information Acts[13;14]. It requires that the appropriate structures and people are put in place within organisations to meet the requirements of the legislation. The legislation applies to public sector and to the private sector only where individuals are providing services as agents to the public sector. It is essentially concerned with conferring rights on individuals to access information held about them and amend it where appropriate.

Guidelines have been produced to assist public bodies in complying with the obligations of the FOI Acts. It is anticipated that the Health Information Bill will further build on these provisions and requirements relating to freedom of information assurance.

9 Conclusion

The aim of this document is to examine and outline the legislative provisions relating to IG and the structures, policies and guidelines that are in place in the Irish health and social care sector. The document explores what is in place under the headings of the six IG topics:

- IG management
- confidentiality and data protection assurance
- information security assurance
- clinical information assurance/care records assurance
- secondary use assurance
- freedom of information assurance.

These topics have been addressed by a number of organisations. At a basic level holders of data strive to comply with the legal requirements conferred on them such as the general provisions set out in the Data Protection and Freedom of Information Acts, and more specifically the legislation relating to the operation of specific organisation such as the NCRI.

Forthcoming legislation in the form of the Health Information Bill signifies a new departure in IG in that it will apply specifically to health information which brings with it its own set of specific requirements.

This "As Is" analysis has demonstrated that much work has been undertaken in respect of IG and pockets of good governance can be identified. However, what has been developed is fragmented and lacks the uniformity that is required to ensure that all health and social care information is recorded, held and managed in a manner that reflects best practice and the interests of patients and service users.

Having completed this "As Is" analysis, in addition to the document *International Review of Information Governance Structures*[8] , the next step for the Authority is to develop high level guidelines around IG. These will be informed by the findings in both of these documents and by consultation with stakeholders. It is intended that these guidelines will support the national standards for health IG to be developed by the Authority, following the enactment of the Health Information Bill.

Appendix 1: Acronyms

CMOD	Centre for Management and Organisation Development
CSO	Central Statistics Office
ESRI	Economic and Social Research Institute
FOI	Freedom of Information
GPIT	General Practice Information Technology
HIPE	Hospital In-Patient Enquiry
HRB	Health Research Board
HSE	Health Service Executive
ICGP	Irish College of General Practitioners
IG	Information Governance
NCRI	National Cancer Registry, Ireland
NIDD	National Intellectual Disability Database

Appendix 2:
Meetings with Stakeholders

Date of Meeting	Organisation
08/07/2009	Health Intelligence Unit, Population Health, HSE
09/07/2009	The National Cancer Registry of Ireland
20/07/2009	Health Intelligence Unit, Population Health, HSE
21/07/2009	Office of the Data Protection Commissioner
21/07/2009	Centre for Management and Organisation Development (CMOD), the Department of Finance
22/07/2009	Health Research Board (HRB), representatives form the disability, drug and mental health information systems units
22/07/2009	Irish College of General Practitioners (ICGP) and General Practice Information Technology (GPIT) Group
23/07/2009	HSE (Information Governance Project Group), including representatives from the ICT Directorate, Consumer Affairs, Quality and Risk and HR
02/09/2009	The Office of the Information Commissioner
02/09/2009	An Bord Altranais (The Nursing Board)
07/10/2009	Department of Health and Children
12/10/2009	The National Health Information Standards Steering Committee (NHISSC)
15/12/2009	The Central Statistics Office

Appendix 3:
Similarities and Differences between Data Protection Acts and Freedom of Information (FOI) Acts

(as outlined in the discussion paper on the proposed Health Information Bill[2])

- FOI does not apply to the private sector except where individuals are providing services as agents to the public sector (for example, GMS GP and medical card patients). Data protection applies to both the public and private sectors
- the FOI Acts do not establish an explicit set of information quality principles applicable to those collecting, keeping, using and disclosing information (personal or otherwise). The DP Acts provide such a framework but only in relation to personal information
- the definition of personal information varies between both Acts
- FOI has no concept of "sensitive" data as found in the DP Acts
- the FOI Acts provide that an individual acting in an official capacity within an organisation is not to be regarded as a third party for privacy protection purposes. This is not the case with the DP Acts
- FOI applies to deceased individuals whereas the DP Acts apply to living identifiable individuals only
- the FOI legislation addresses the position of children explicitly. The DP legislation does not
- the FOI Acts have express provisions about helping people with subject access requests. The DP Acts do not
- there is no upfront fee payable under FOI for access by an individual to his or her personal information. There is a maximum fee of €6.35 payable under the DP Acts
- there is a specific provision in the Data Protection Act 2003 (Section 1(5)(a)) that "a right conferred by this Act shall not prejudice the exercise of a right conferred by the Freedom of Information Act 1997"
- the length of time for complying with an access request varies – 20 days under FOI and 40 days under DP
- both FOI and Data Protection legislation contain express references to subject access to health related data but vary in the applicable rules.

Reference List

References

(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 Department of Health and Children. *The National Health Information Strategy*. 2004.

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

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

(7) *The Health Act* 2007.

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

(9) 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

(10) NHS Connecting for Health. *Information Governance Toolkit - Derivations and Support for Standards*. 2007. Available from: URL: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/v5derivations.pdf. Accessed: 16 Sep 2009

(11) *The Data Protection Act* 1988.

(12) *The Data Protection (Amendment) Act* 2003.

(13) *The Freedom of Information Act* 1997.

(14) *The Freedom of Information (Amendment) Act* 2003.

(15) *Bunreacht na hEireann* 1937.

(16) The Council of Europe. *Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data*. 1981. Available from: URL: http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm. Accessed: 31 Aug 2009

(17) The Office of the Data Protection Commissioner. *Data Protection (Amendment) Act 2003 - A Summary Guide*. 2003. Available from: URL: http://www.post.trust.ie/images/New_Act_Summary_website_version.pdf. Accessed: 31 Aug 2009

(18) The National Hospitals Office. *Code of Practice for Healthcare Records Management*. 2007. Available from: URL: http://213.94.192.205/en/Publications/HSEPublicationsNew/AcuteHospitalReportsGuidelines/NHOCodeofPracticeonHealthcareRecords/FiletoUpload,6884,en.pdf. Accessed: 31 Aug 2009

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

(20) The Office of the Data Protection Commissioner. *Statement of Strategy 2009-2010*. 2008. Available from: URL: http://www.dataprotection.ie/viewdoc.asp?DocID=904&ad=1#1. Accessed: 31 Aug 2009

(21) Office of the Data Protection Commissioner. *Data Protection Audit Resource*. 2009. Available from: URL: http://www.dataprotection.ie/viewdoc.asp?DocID=894&m=f. Accessed: 21 Oct 2009

(22) *Data Protection (Access Modification) (Health) Regulations* 1989.

(23) FOI Central Policy Unit, The Department of Finance. *A Short Guide to the Freedom of Information Act 1997 and Freedom of Information (Amendment) Act 2003*. 2004. Available from: URL: http://www.foi.gov.ie/short-guide-to-the-foi-acts. Accessed: 9 Sep 2009

(24) The Department of Health and Children. *Cancer Services in Ireland: A National Strategy*. 1996.

(25) 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*. June 2008. Available from: URL: http://www.dohc.ie/consultations/closed/hib/draft_audit_paper.pdf?direct=1. Accessed: 31 Aug 2009

(26) The Office of the Data Protection Commissioner. *Ninth Annual Report of the Data Protection Commissioner*. 1997.

(27) *Health (Provision of Information) Act* 1997.

(28) The National Cancer Registry, Ireland. *Data Confidentiality in the National Cancer Registry - General policy, procedures for release of data and staff guidelines*. 2007. Available from: URL: http://ncri.ie/data.cgi/html/NCRI-data-confidentiality.rtf. Accessed: 4 Sep 2009

(29) *The Disability Act* 2005.

(30) The Department of Justice, Equality and Law Reform. *Guide to the Disability Act 2005*. 2005. Available from: URL: http://www.justice.ie/en/JELR/DisabilityAct05Guide.pdf/Files/DisabilityAct05Guide.pdf. Accessed: 5 Nov 2009

(31) *The Statistics Act* 1993.

(32) *The Social Welfare Act* 1998.

(33) *The Social Welfare and Pensions Act* 2005.

(34) *Social Welfare (Miscellaneous Provisions) Act* 2002.

(35) *The European Convention on Human Rights Act* 2003.

(36) *The Human Rights Commission Act* 2000.

(37) The Council of Europe. *Convention for the Protection of Human Rights and Fundamental Freedoms*. 2003. Available from: URL: http://www.echr.coe.int/nr/rdonlyres/d5cc24a7-dc13-4318-b457-5c9014916d7a/0/englishanglais.pdf.

(38) *EU Directive 95/46/EC - The Data Protection Directive* 1995.

(39) *Nurses Act* 1985.

(40) An Bord Altranais. *The Code of Professional Conduct for each Nurse and Midwife*. 2000. Available from: URL: http://www.lenus.ie/hse/handle/10147/44988. Accessed: 10 Sep 2009

(41) An Bord Altranais. *Guidance to Nurses and Midwives Regarding Ethical Conduct of Nursing and Midwifery Research*. 2007. Available from: URL: http://209.85.229.132/search?q=cache:y37LM1DsUIkJ:www.nursingboard.ie/GetAttachment.aspx%3Fid%3D322b92ac-60f6-48c6-8ec6-88c087a8013f+guidance+to+nurses+and+midwives+regarding+ethical+conduct+of+nursing+and+midwifery+research&cd=1&hl=en&ct=clnk&gl=ie. Accessed: 10 Sep 2009

(42) *The Medical Practitioners Act* 1978.

(43) The Medical Council. *Guide to Professional Conduct and Ethics for Registered Medical Practitioners*. 2009. Available from: URL: http://www.medicalcouncil.ie/_fileupload/misc/171109%20Final%20Version%20Ethics%20Guide%20Update%20For%20Printer.pdf. Accessed: 8 Dec 2009

(44) *The Medical Practitioners Act* 2007.

(45) The Organisation for Economic Cooperation and Development. *OECD Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data*. 1980. Available from: URL: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. Accessed: 31 Aug 2009

(46) The National FOI/DP Liaison Officers Group. *Freedom of Information Acts 1997 and 2003, Data Protection Acts 1988 and 2003 and Administrative Access Policy - A Practical Guide for Staff*. 2004.

(47) Health Intelligence Unit, HSE. *Health Intelligence Initiatives - Population Health, Knowledge Management and Health Informatics*. 2009. Available from: URL: http://www.hse.ie/eng/Publications/corporate/metr/Health_Intelligence_Supplement_Pages_72-96.pdf. Accessed: 9 Sep 2009

(48) The Health Service Executive. *Quality and Risk Management Standard*. 2007. Available from: URL: http://www.hse.ie/eng/About_the_HSE/Whos_Who/Quality_and_Risk_Management.html. Accessed: 16 Sep 2009

(49) The Irish College of General Practitioners and the National General Practice Information Technology Group. *Managing and Protecting the Privacy of Personal Health Information in Irish General Practice*. 2003. Available from: URL: http://www.icgp.ie/go/in_the_practice/information_technology/publications_reports. Accessed: 4 Sep 2009

(50) The National Intellectual Disability Database Committee in association with the Department of Health and Children and Inclusion Ireland. *Planning Services for People with Disabilities - A Guide to the Intellectual Disability Database*. 2006.

(51) The Health Research Board. *National Intellectual Disability Database - Software Support*. 2009. Available from: URL: http://www.hrb.ie/health-information-in-house-research/disability/nidd/software-support/. Accessed: 2 Dec 2009

(52) The Health Research Board. *Requesting Information from the National Intellectual Disability Database*. 2009. Available from: URL: http://www.hrb.ie/health-information-in-house-research/disability/nidd/accessing-information/. Accessed: 2 Nov 2009

(53) The Centre for Management and Organisation Development (CMOD), the Department of Finance. *Protecting the Confidentiality of Personal Data - Guidance Note*. 2008. Available from: URL: http://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf. Accessed: 4 Sep 2009

(54) The Office of the Data Protection Commissioner. *Data Protection Acts 1988 and 2003 - A Guide for Data Controllers*. 2008. Available from: URL: http://www.dataprotection.ie/documents/forms/NewAGuideForDataControllers.pdf. Accessed: 31 Aug 2009

(55) Sheikh, A. Commissioned by the HRB. *The Data Protection Acts 1988 and 2003: Some implications for public health and medical research - a discussion document*. 2008. Available from: URL: http://www.hrb.ie/research-strategy-funding/publications/rsf-publication/publications//411/. Accessed: 5 Nov 2009

(56) The Information Sharing Framework Working Group. *Interim Guidelines on Information Sharing in Primary Care Teams*. 2008.

(57) The National GPIT Group. *No Data, No Business: Information Communication Technology (ICT) Security Guidelines*. 2008. Available from: URL: http://www.icgp.ie/go/in_the_practice/information_technology/news_updates/E3E7417C-19B9-E185-833C5534D98B3B8C.html. Accessed: 8 Sep 2009

(58) The Office of the Data Protection Commissioner. *Data Protection Guidelines for Developing Security Policies*. 2008. Available from: URL: http://dataprotection.ie/viewdoc.asp?m=&fn=/documents/responsibilities/sg160204.htm. Accessed: 11 Sep 2009

(59) The Office of the Information Commissioner. *Records Management Handbook*. 2004. Available from: URL: http://www.oic.gov.ie/en/Publications/OfficeManuals/RecordsManagementHandbook/. Accessed: 16 Sep 2009

(60) An Bord Altranais. *Recording Clinical Practice Guidance to Nurses and Midwives*. 2002. Available from: URL: http://www.lenus.ie/hse/handle/10147/45061. Accessed: 10 Sep 2009

(61) FOI Central Policy Unit, The Department of Finance. *Manual for Freedom of Information Decision Makers*. 2004. Available from: URL: http://www.foi.gov.ie/decision-makers-manual. Accessed: 10 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