

**AUDIT OF KEY INTERNATIONAL INSTRUMENTS,
NATIONAL LAW AND GUIDELINES RELATING
TO HEALTH INFORMATION FOR IRELAND AND
SELECTED OTHER COUNTRIES**

**Prepared in conjunction with the
Discussion Paper on the
Health Information Bill**

June 2008

AUDIT

Introduction

As part of the Health Reform Programme, the Department of Health is preparing a Health Information Bill which will assist with creating a new framework to facilitate the best use of personal health information for enhanced patient care and for the better management of health services generally. The new framework will also provide the legal basis for the implementation of modern information technologies to assist with that goal.

This Audit Paper (which accompanies the more extensive and complementary Discussion Document) is part of the consultation process designed to ensure that matters relevant to the Health Information Bill are identified and properly considered.

In considering this Audit, especially those sections that examine the law and practice in other jurisdictions, it is very important to bear in mind that every country's health system is uniquely shaped by a particular range of historical, cultural, social, political and economic factors. Further, a country's health system, at any point in time, is always evolving and generally reflects wider contemporary values and priorities in society. Accordingly, what works well in one jurisdiction may not work so well in another.

Notwithstanding the above, there is widespread agreement that better healthcare information systems and e-health technologies can support more efficient and effective health services. Similarly, there is also international consensus on the need to protect the privacy and confidentiality of patient information and to safeguard it from inappropriate collection, use, disclosure and linkage.

The Audit is structured as follows: Part 1 looks at international initiatives in the areas of privacy, human rights and data protection, (ii) Part 2 examines Irish sources of law and practice affecting personal health information and (iii) Part 3 looks at the position in other countries. The Appendix provides an overview, distilled from international law and practice, of generally accepted principles in the handling of personal health information. The emphasis in the Audit is on legal and official documents and sources.

June 2008

CONTENTS

	Page
EXECUTIVE SUMMARY	3
PART 1: INTERNATIONAL INSTRUMENTS	5
PART 2: IRELAND	10
PART 3: OTHER COUNTRIES	17
APPENDIX: GENERALLY ACCEPTED PRINCIPLES FOR HANDLING PERSONAL HEALTH INFORMATION	27

EXECUTIVE SUMMARY

Part 1 looks at the major international instruments, treaties and agreements relevant to privacy and the protection of confidentiality of health information. It traces the evolution from concern with privacy generally in instruments such as the *Universal Declaration on Human Rights (1948)* and *European Convention on Human Rights and Fundamental Freedoms (1950)* to a more particular concern with information privacy, as for example, in the *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (1981)*. This increase in concern with information privacy was driven primarily by the recognition of the power of new technologies to process and profile vast amounts of personal information in a way that was never previously possible.

The European Union has also taken a major interest in information privacy and its 1995 Directive on Data Protection (95/46/EC) introduced a minimum floor of rights for individuals in relation to their personal information in Member States while at the same time facilitating the completion of the Internal Market.

Both the 1981 Convention and 1995 Directive identified personal health information as sensitive and deserving of special protection.

Part 2 looks at Ireland and focuses on:

- National Law,
- Professional Ethical Codes,
- Health Strategies and Reports, and
- Other Reports, Books and Guides.

Under the National law heading, there is consideration of the relevant Constitutional cases, the common law duty of confidence which is applicable to medical practitioners, and legislation that impacts upon the management of information in the health sector. There are a number of important statutes, the most significant of which are the *Freedom of Information Acts 1997 and 2003* and the *Data Protection Acts 1988 and 2003*.

Ethical codes for healthcare professionals are also an important part of the regulatory environment in Ireland. These codes provide guidance on matters such as the confidentiality that attaches to medical records and the importance of patient consent to third party disclosure.

The present regulatory framework operates within a major ongoing health reform programme. The reports and strategies that underpin that programme, such as *Quality and Fairness -the National Health Strategy (2001)* provide a context for understanding the policy objectives that will drive a Health Information Bill.

There is also a consideration of other Irish reports, publications and official guides that help provide a better understanding of the overall structure which governs the management of personal health information in Ireland.

Part 3 is concerned with considering the regulation of personal health information in certain other countries and at EU level. The countries are Canada, New Zealand, Australia and the United Kingdom. What emerges are the similarities in terms of general principles and differences in certain areas, such as rules on health research. Canada and Australia, for example, have wide-ranging Privacy Acts at Federal and Commonwealth level respectively while most of the individual Provinces and States have legislation dealing specifically with health information. The United Kingdom, like Ireland, has given effect to the 1995 EU Directive but there are different rules on using patient information for research in England and Wales, on the one hand, and Scotland on the other. Notwithstanding any variations or differences between EU Member States on the implementation of the 1995 Directive, the 2006 EU funded EuroSOCAP study - ***European Standards on Confidentiality and Privacy in Healthcare***- found that there are a number of shared legal principles on using and disclosing patient information throughout the Union which emphasised respect for confidentiality as the key factor.

Part 1: INTERNATIONAL INSTRUMENTS and EU DIRECTIVE

There are a range of international declarations, treaties and agreements relevant to the area of protecting 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. The most important of these international instruments are:

International Privacy and Human Rights Instruments

Universal Declaration on Human Rights (1948) ~ Adopted and proclaimed by the United Nations General Assembly resolution 217 A (III) of 10 December 1948. It is an advisory declaration consisting of 30 Articles which outline the view of the United Nations General Assembly on the human rights guaranteed to all people. Article 12 addresses privacy: ‘No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks’.

European Convention on Human Rights & Fundamental Freedoms (1950) ~ The ECHR is an international treaty which is binding on all those countries that have ratified it, which includes all EU Member States.¹ The Convention established the European Court of Human Rights. Any person who feels their rights have been violated under the Convention by a State party can take a case to the Court; the decisions of the Court are legally binding, and the Court has the power to award damages. Article 8 deals with privacy and states that:

“(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except as 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 case law of the European Court of Human Rights (ECtHR) makes clear that the essential object of Article 8 is to protect the individual against arbitrary interference by the public authorities. There are, in addition, obligations on States to take positive steps to ensure that the Article 8 right is respected, not merely to avoid measures which interfere with the right.

The ECtHR has held: ‘Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the

¹ Ireland ratified the Convention in 1953. The European Convention on Human Rights Act (No.20 of 2003) brought the Convention into Irish law subject to the Constitution.

medical profession and in the health services in general. Without such protection, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment, and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community' (*Z v Finland* 1997; *MS v Sweden*, 1997).

International Covenant on Civil & Political Rights (1966) ~ This Covenant is a legally binding United Nations treaty based on the Universal Declaration of Human Rights, created in 1966 and entered into force in March 1976. Ireland ratified the Covenant in December 1989. Article 17 states: 'No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference.'

Charter of Fundamental Rights of the EU (2000) (2000/C 364/01) ~ The Charter does not cover 'new' rights but rather sets out again, in a clear and concise form, a wide range of fundamental rights applicable to the EU. At present, the Charter does not enjoy unequivocal legal status but it is intended that it should. Two articles of the Charter emphasize the importance of the protection of privacy: Article 7 states:

'Everyone has the right to respect for his or her private and family life, home and communications.'

Article 8 states:

'1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.'

The Charter will have legal effect if the 2007 draft ***EU Reform Treaty*** is adopted.

Universal Declaration on Bioethics and Human Rights (2005) ~ The Declaration puts human rights at the heart of bioethics and upholds human dignity, human rights and fundamental freedoms in scientific research, medical practices and the development of technologies. *Article 9 provides:*

'The privacy of the persons concerned and the confidentiality of their personal information should be respected. To the greatest extent possible, such information should not be used or disclosed for purposes other than those for which it was collected or consented to, consistent with international law, in particular international human rights law.'

There are also the related Declarations on the Human Genome and Human Rights and on Human Genetic Data.

Council of Europe ‘Convention for the Protection of Human Rights and Dignity of the Human Being with Regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine’ (No. 164) (1997).

The Convention on Human Rights and Biomedicine expands on many of the rights contained in the European Convention on Human Rights and elaborates how they apply in the field of medicine. Unlike the ECHR which applies to all EU Member States, the Convention on Human Rights and Biomedicine has not been signed or ratified by many States, including most of the larger States. In spite of it not applying directly to many EU States, it is nevertheless significant in that it has been drawn upon by the European Court of Human Rights in making judgments involving States who are not parties to this Convention. Article 10 of the Convention on Human Rights and Biomedicine states:

- (1) Everyone has the right to respect for private life in relation to information about his or her health.
- (2) Everyone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed.
- (3) In exceptional cases, restrictions may be placed by law on the exercise of the rights contained in paragraph 2 in the interests of the patient.

The 2005 ‘***Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research***’ (No. 195) (2005) also emphasizes the importance of confidentiality. Article 25 (1) states that:

‘Any information of a personal nature collected during biomedical research shall be considered as confidential and treated according to the rules relating to the protection of private life.’

International Data Protection Instruments

The two major – and broadly similar – international data protection instruments are:

- ◆ The Organisation for Economic Co-operation & Development’s 1980 Guidelines Governing the Protection of Privacy & Transborder Flows of Personal Data (adopted on 23 September 1980).
- ◆ The Council of Europe’s 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.

Both of the above address information privacy issues in the context of the economic value associated with the free flow of information across national borders. This is something that also arises in the subsequent 1995 EU Directive on Data Protection (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 Directive, personal health

information is identified as sensitive and therefore deserving of additional protection.

OECD Guidelines

The Preface to the OECD Guidelines Adopted on 23 September 1980 states that “the development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data.”

It goes on to say that:

“... although national laws and policies may differ, member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information.”

The Guidelines explicitly recognized that limiting the relevant rules solely to the computerised processing of personal data could have drawbacks.

Council of Europe Data Protection Convention (1981)

The 1981 Council of Europe Data Protection Convention (No. 108) extended the protection granted to confidentiality by the ECHR. This Convention was the first international legally binding text on data confidentiality. It applies to all ‘automated personal data files and automatic processing of personal data in the public and private sectors’ (Article 3), as long as the data relates to an ‘identified or identifiable individual’ (Article 2), whatever their nationality or place of residence. The (Irish) Data Protection Act 1988 was based on the principles in the Convention.

There are also two (non-binding) information related Council of Europe Recommendations relevant to the health sector adopted by the Council of Europe. They address *medical databanks*² and the protection of *medical and genetic data*³. The first introduced the notion that subject access to personal health information might be handled through a physician rather than directly by the patient. It also developed the idea that erroneous patient information might still be retained in the record held, even after the correct information came to light, and would be retained because the incorrect information might have had some bearing on treatment received, etc. The erroneous nature of such information, and the reason for its retention, would, however, have to be clearly marked within the record. The second recommendation on genetic data updated the medical databanks’ recommendation the light of developing trends and of the increasing use of genetic data.

² Council of Europe Recommendation, R(81)1, on *Automated Medical Databanks*.

³ Council of Europe Recommendation, R(97)5, on the *Protection of Medical Data*.

EU Initiatives on Data Protection

Directive on Data Protection (95/46/EC)

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. 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-inforced 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 was to implement the Directive in Ireland.

Article 8 of the Directive deals with the processing of special categories of data. Health information is expressly recognized as one of the sensitive categories. Member States must prohibit the processing of those special categories of data, except in the situations:

- (a) where the data subject has given his or her explicit consent;
- (b) where the processing is necessary to protect the vital interests of the data subject or of another person;
- (c) where the data subject is physically or legally incapable of giving consent.
- (d) where 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
- (e) where, 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.

Part 2: IRELAND

In this Part, the Audit focuses on

- National Law
- Professional Ethical Codes
- Health Strategies and Reports
- Other Reports, Books and Guides

National Law

Relevant here are-

- the Constitution,
- Data Protection and Freedom of Information Legislation, and
- Common Law Duties of Confidentiality.

The Constitution

Ireland has a written Constitution (Bunreacht na hEireann) enacted by the people and capable of being amended only by the people through a referendum. It contains a number of explicit enumerated personal rights which have been supplemented by judicial interpretations –the so-called unenumerated rights.

Although there is not an express reference to a right to privacy in the Irish Constitution, the Supreme Court has ruled an individual may invoke the personal rights provision in Article 40.3.1 to establish an implied right to privacy. This article provides that:

“... the State guarantees in its laws to respect, and, as far as practicable, by its laws to defend and vindicate the personal rights of the citizens.”

It was first used to establish an implied constitutional right in the case of *McGee v. Attorney General*⁴ which recognised the right to marital privacy. This case was followed by others, such as *Norris v. Attorney General*⁵ and *Kennedy v. Ireland*⁶. In the *Kennedy Case*, the Supreme Court held that:

“... the right to privacy is one of the fundamental personal rights of the citizen which flow from the Christian and democratic nature of the State ... The nature of the right to privacy is such that it must ensure the dignity and freedom of the individual in a democratic society. This can not be insured if his private communications, whether written or telephonic, are deliberately and unjustifiably interfered with.”

⁴ *McGee v. Attorney-General* [1974] I.R. 284.

⁵ *Norris v. Attorney General* [1984] I.R. 36.

⁶ *Kennedy v. Ireland* [1987] I.R. 587.

In the same case, the then High Court judge (later Chief Justice), Mr Justice Liam Hamilton, added:

“... the right of privacy ... is not an unqualified right. Its exercise may be restricted by the Constitutional rights of others, by the requirements of the common good and it is subject to the requirements of public order and morality ...The nature of the right to privacy must be such as to ensure the dignity and freedom of an individual in the type of society envisaged by the Constitution, namely a sovereign, independent and democratic society.”

Legislation

Legislation or statute law can be divided into primary and secondary legislation. The former passes through the Oireachtas as a Bill before being signed by the President and becoming an Act. Secondary legislation derives from provisions in Acts allowing for Ministerial Orders and Regulations to be made in matters germane to the statute.

The main Acts relevant to health information management are:

- Data Protection Acts 1988 & 2003
- Freedom of Information Acts 1997 & 2003
- Health Act 2007
- Disability Act 2005
- European Convention on Human Rights Act 2003
- Statistics Act 1993
- Social Welfare Acts 1998 and 2002

Data Protection Acts 1988 & 2003 and Freedom of Information Acts 1997 & 2003

These are discussed in detail in the Discussion Document

Health (Provision of Information) Act 1997

This legislation was introduced to facilitate the development of the National Cancer Registry of Ireland. The Act essentially provides exemption for specified parties from the disclosure provisions of the Data Protection Acts for certain information released to the Registry. It does not, however, deal with the duty of confidence obligations.

Disability Act 2005

This Act introduced a series of provisions dealing with genetic data and testing. The Act also contains –in Section 41- a definition of “genetic data” as data relating to a living person derived from genetic testing of the person.

The provisions aim to ensure that people who may be affected by genetic disorders will not be subject to any unreasonable 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. These new safeguards will be reviewed no later than 2014.

The safeguards provide that –

- genetic testing may only take place with a person’s consent, in accordance with the Data Protection Acts
- the results of a genetic test can’t 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
- the use of a person’s family history for insurance purposes may be regulated by the Minister after consultation with other relevant Ministers, the Data Protection Commissioner and other interested bodies or groups.

Health Act 2007

The 2007 Act which established the Health Information and Quality Authority and conferred certain information related functions on it as per the National Health Information Strategy (2004).

Statistics Act 1993

This legislation provides a statutory basis for the collection and use of specified information, including health information, and allow for outside parties to be designated, under the Acts, for the purposes of carrying out certain research on the information collected. (Reference has already been made to the European Convention on Human Rights Act 2003.)

Social Welfare Acts 1998 and 2002

The Social Welfare Act 1998, as well as introducing the Personal Public Service Number as being obligatory for the receipt of publicly funded services, also introduced the concept of a Public Service Card which has relevance to the design of any unique health identifier. The Social Welfare (Miscellaneous Provisions) Act 2002 introduced the concept of a public service identity which again would have relevance to any proposed identification system within the Health Service.

European Convention of Human Rights Act 2003

This statute incorporated the Convention into Irish law. Under the Act, Irish courts are required to interpret Irish law in line with the Convention rather than directly apply its provisions.⁷

Common Law 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. At common law, the duty of confidence is very relevant to

⁷ This means that when someone is faced with a particular legal provision which he or she believes contravenes his or her rights under the Convention, rather than asking the Court to invalidate the provision in light of the conflicting convention right, he or she must ask a court to interpret the provision in line with the convention.

personal health information. For doctors, the duty is founded on the ethical duty of medical confidentiality which derives from the *Hippocratic Oath*⁸ and has been re-affirmed in the *Declaration of Geneva*⁹, the *International Code of Medical Ethics* (1949) and most codes of professional conduct worldwide. (Ethical codes in Ireland are discussed below.)

In the leading Irish case of *House of Spring Gardens v Point Blank Limited*¹⁰, Costello J. said that an action for breach of confidence must consist of the following elements: (i) there must exist (from the relationship between the parties) an obligation of confidence regarding the information which had been imparted; (ii) the information which had been communicated must properly be regarded as confidential; (iii) the recipient of the information must have breached his or her duty to act in good faith (that is, he or she must have used the information for a purpose for which it was not imparted to him and to the detriment of the informant).

On the basis of the above, 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.

Professional Ethical Codes

It is not, therefore, surprising that most healthcare professionals' associations stress ethical considerations especially when it comes to patients and their medical records. For doctors, these are set out in *A Guide to Ethical Conduct and Behaviour*¹¹. That Code emphasises the importance – “a time-honoured principle”- of the duty of confidence (even after death) that exists between the doctor and the patient and the accompanying obligation on the clinician not to disclose what he or she has been told except with patient consent. The following exceptions are recognised:

- when ordered by a Judge in a Court of Law or by a Tribunal established by an Act of the Oireachtas,
- when necessary to protect the interests of the patient,
- when necessary to protect the welfare of society,
- when necessary to safeguard the welfare of another individual or patient.

Nurses are similarly bound by their own Code prepared by An Board Altranais (Irish Nursing Board) - *The Code of Professional Conduct for each Nurse and Midwife*¹² which provides that the confidentiality of patients' records must be safeguarded.

⁸ The Oath states that ‘what I may see or hear in the course of treatment I will keep to myself holding such things shameful to be spoken about’.

⁹ World Medical Council Declaration of Geneva, 1947

¹⁰ [1984] IR 611; See also *Cook v Carroll* [1945] IR 515

¹¹ Irish Medical Council, 6th edition (2004). The Code is currently being reviewed by the Medical Council.

¹² Irish Nursing Board (April 2000)

As regards other healthcare professions, the Health and Social Care Professionals Act 2005 provided, inter alia, for registration boards for certain designated health and social care professions. A number of those designated professions also have ethical codes dealing with the privacy and confidentiality of patient information. For example, the Psychological Society of Ireland *Code of Professional Ethics*¹³ and the Association of Occupational Therapists of Ireland's *Code of Ethics and Professional Conduct for Occupational Therapists*¹⁴.

European wide perspectives on health information and confidentiality are discussed in Part 3 of this Review.

Healthcare Strategies and Reports

As the proposed Health Information Bill is a part of the Health Reform Programme, the reports and strategies underlying that programme are directly relevant. All the reports identified the critical need for much improved information systems if reform goals were to be achieved. That imperative was set out most clearly in the National Health Information Strategy (2004) as were the related issues of privacy, confidentiality and security of patient information. The principal reports were:

- **Audit of Structures and Functions in the Health System** (the “Prospectus Report”)
- **Report of the Commission on Financial Management and Control Systems in the Health Service** (the “Brennan Report”) and
- **Report of the Taskforce on Medical Staffing** (the Hanly Report).

The main strategies were:

- *Quality and Fairness, A Health System for You* (the National Health Strategy) (2001),
- *Primary Care: New Direction* (the Primary Care Strategy) (2001) and
- *Health Information: A National Strategy* (the National Health Information Strategy) (2004).

References to the role of information technology in healthcare are also found in the current national social and economic agreement, *Towards 2016*, and the *National Development Plan 2006-13*.

Other Reports, Books and Guides

The Annual Reports of the Information Commissioner and the Data Protection Commissioner frequently features cases and comments on the application, impact and problems associated with health information in their respective areas of responsibility. Much of that comment calls for greater awareness and compliance. The websites of the

¹³ Psychological Society of Ireland 3rd revision (1999)

¹⁴ Association of Occupational Therapists of Ireland

Commissioners are an extremely useful resources for up-to-date information especially in relation to case and court decisions.¹⁵ In that regard, their respective websites indicate that there have been many more formal Commissioner determinations and judicial decisions under the FOI Acts than under the longer established Data Protection Acts.

In the area of health research, there is a national strategy in place – ***Making Knowledge Work for Health: A Strategy for Health Research***¹⁶ – in place since 2001. The Strategy reflects the view that knowledge-based innovation and new ways of thinking are required for the future development of the health services, if continued health and social gain are to be realised. From the information privacy perspective, two factors were expressly identified as hindering research in the Irish health system:

- the absence of a unique national patient / client identifier
- the implications of data protection law for the creation and maintenance of population databases and registries.

The Data Protection Commissioner has also considered the matter of research and has produced –after a consultation period- ***Guidelines on Research in the Health Sector***¹⁷. The document distinguishes between in-house and third party research and places considerable emphasis on the need for consent in the case of the latter.

The only specific information guide relevant to the health sector prepared to date (and with the support of the Data Protection Commissioner) is the joint National GPIT Group, Irish College of General Practitioners and Irish Medical Organisation ***Guide to Managing and Protecting Personal Health Information in Irish General Practice***.¹⁸ The Guide was prepared specifically for use by general practitioners and indicates how they should manage patient information within the regulatory environment of laws and ethical codes. As general practice is at the heart of a considerable amount of patient information flows between different parts of the health system, the guide pays considerable attention to the rules governing such communications.

There is also the staff guide prepared in 2005 by the Health Service Executive ***Personal Information – its collection, use and distribution: A Handbook for Health Service Executive Staff***.¹⁹ The handbook looks at the relevant law and advises on best practice for HSE staff in complying with the law both in terms of sharing information within the organisation and with persons outside of it.

The only published book to date in this area in Ireland is ***Protecting Personal Health Information in Ireland: Law and Practice***²⁰ which looks at the development of data protection law in Ireland in an international context and how it currently operates in the

¹⁵ Data Protection Commissioner website is www.dataprivacy.ie and the Freedom of Information Commissioner's website is www.oic.ie

¹⁶ Department of Health & Children (2001)

¹⁷ Data Protection Commissioner (November 2007)

¹⁸ P.Lennon, Dr B Meade and Dr R Boland (2005)

¹⁹ HSE (2005)

²⁰ Peter Lennon (Oak Tree Press) (2005)

health system. It sees the major issue as one of reconciling increasing claims for use and disclosure of health information against long established patient rights to control their information.

The leading textbook on the Irish Constitution is *JM Kelly: The Irish Constitution*²¹ which traces the evolution of the concept of privacy, as an implied right, in the Irish courts beginning with the right to marital privacy and the subsequent widening of the judicial recognition. There is also the Law Reform Commission Study *Report on Privacy: Surveillance and the Interception of Communications*²² which looks at long held privacy notions against the backdrop of the increasing citizen surveillance found in modern society. The Commission remarked that “many countries, including Ireland, have a web of laws that protect isolated aspects of privacy. A few countries, mainly European, have tailor-made privacy laws that adequately protect privacy in the round and directly.” The LRC commented on the lack of comprehensive or effective legal protection as a matter of “growing public concern”. It also acknowledged that defining privacy had always proved difficult but offered the following description “...at its core lies the desire of the individual to maintain control over information...and as a corollary to deny or control access thereto by others...”

Two important studies are the Irish Council for Bioethics report on *Human Biological Material: Recommendations for Collection, Use & Storage in Research*²³ and the Health Research Board’s *Public Perceptions of Biomedical Research: A Survey of the General Population in Ireland*²⁴. The Irish Council’s report devotes considerable attention to the issue of consent and, while the matter is discussed primarily with regard to participation in the research exercise rather than the processing of a participant’s personal information per se, it is clear that similar consent principles apply to the latter as to the former. The report also deals explicitly with confidentiality and privacy. The HRB study included the finding that “the introduction of privacy legislation mandating informed consent for access by researchers to medical records has adversely affected cancer registries in England and Germany”.

²¹ GW Hogan & GF Whyte (Butterworths) 4th Edition.

²² (LRC 57–1998)

²³ Irish Council for Bioethics (2005)

²⁴ Health Research Board (2005)

Part 3: OTHER COUNTRIES

Ireland is not alone in seeking to address the issues posed by the desire to have a modern efficient, effective, value for money and patient centred health service. Other countries have also sought to maximize modern information system for the benefit of individual patients and the health system generally. For that reason, the experience in other countries and the perspective at European are worth examining subject to the caveat in the Introduction to this Audit Paper that what works well in one country many not be so appropriate or effective in another.

CANADA

Legislation -Canada has two federal privacy laws, the Privacy Act 1980 and the Personal Information Protection and Electronic Documents Act 2000. Oversight of both Federal Acts rests with the Privacy Commissioner of Canada who is authorized to receive and investigate complaints.

The Privacy Act imposes obligations on federal government Departments and agencies to respect privacy rights by limiting the collection, use and disclosure of personal information. Individuals are also protected by the Personal Information Protection and Electronic Documents Act (PIPEDA) that sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. Both Acts give individuals the right to access and request correction of the personal information these organizations may have collected about them.

A constitutional right to information privacy is slowly being developed in Canada. This is discussed in *Constitutional Law of Canada*²⁵ which points out that the Supreme Court of Canada has specifically recognised the importance of protecting the privacy of personal information in medical or psychotherapy records. The Court intended to safeguard to 'biographical core of personal information' by granting the individual control over the dissemination of this information at the point of disclosure.

While there is no federal health information legislation, the Canadian Medical Association has produced a widely used sectoral code - **Health Information Privacy Code**- and, at province level, several provinces have enacted legislation to deal specifically with the collection, use and disclosure of personal health information by health care providers and other health care organizations.

Alberta (Health Information Act 1999)

The Health Information Act was passed by the Alberta Legislature in 1999 and came into effect in April 2001. It provides individuals with the right to request access to health records in the custody or under the control of custodians, while providing custodians with a framework within which they must conduct the collection, use and disclosure of health information. (Custodians are defined to include: any health service provider paid in part

²⁵ Peter W. Hogg, 3rd edition vol. 2

or in whole by the Alberta Health Care Insurance Plan, pharmacies and pharmacists regardless of how they are paid, nursing home operators etc.)

The Health Information (Amendment) Act 2006 was introduced to address technical enhancements to provincial electronic health records, clarify disclosure rules, improve the Department of Health's capacity to monitor drug trends, and enhance the privacy of Albertans' health information.

Manitoba (Personal Health Information Act 1997)

The Act provides individuals with the right to have their personal health information kept private and to access it when that information is held by a health care provider, health care facility or public body (referred to in the Act as "trustees").

Saskatchewan (Health Information Protection Act 1999)

This Act protects personal health information in the health system in Saskatchewan and establishes a common set of rules that emphasize the protection of privacy, while ensuring that information is available to provide efficient health services.

Ontario (Personal Health Information Protection Act 2004)

The Act governs the manner in which personal health information may be collected, used and disclosed within the health care system. It is very similar to PIPEDA.

Speeches –Successive Privacy Commissioners of Canada and senior members of the Office have made numerous speeches on the subject of privacy and healthcare. The following speeches (all available on the Commissioner's website) illustrate the Office's thinking about the nature of the challenge faced in protecting health information in the modern age while successfully reaping the benefits of the new information technologies.

Protecting Genetic Information in Health Research: The Canadian Approach

Data Protection and Biomedical Research Forum, Address by Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada, Barcelona, Spain, April 25, 2007

Here, Now & Beyond: Protecting Privacy in an Electronic Health Record World

Third Annual Conference on Electronic Health Records and Information Systems, Address by Patricia Kosseim, General Counsel, Toronto, Ontario, November 28, 2006

Legal and Practical Challenges of Protecting Privacy in an EHR World

Electronic Health Information and Privacy Conference, Address by Patricia Kosseim, General Counsel Ottawa, Ontario, November 13, 2006

The Advent of Electronic Health Records (EHRs) in the Current Legal and Policy Context

Electronic Health Information & Privacy Conference, Ottawa Centre for Research and Innovation, Address by Patricia Kosseim, General Counsel, Ottawa, Ontario November 30, 2005

Health Information Privacy

4th Annual Health Information Privacy Conference, Address by Patricia Kosseim, General Counsel, Toronto, Ontario, January 17, 2005

Privacy Laws & Health Information: Making it Work

Privacy Laws & Health Information Conference, Address by Jennifer Stoddart, Privacy Commissioner of Canada, Regina, Saskatchewan, October 27, 2004

Privacy in Health Research: Sharing Perspectives and Paving the Way Forward

Address by George Radwanski, Privacy Commissioner of Canada, November 14, 2002

Genetic Information and the Right to Privacy

Meeting New Standards for Managing Privacy of Health Information, Canadian Institute, Toronto, Ontario, George Radwanski, Privacy Commissioner of Canada, June 18, 2001

Condition Critical: Health Privacy in Canada Today

E-Health 2001: The Future of Health Care in Canada Conference, Toronto, Ontario
George Radwanski, Privacy Commissioner of Canada, May 29, 2001

Studies- A major study on Electronic Health Records was funded by the Privacy Commissioner and carried out by the Universities of Alberta and Victoria in 2005. The published report was entitled *Electronic Health Records and the Personal Information Protection and Electronic Documents Act*.²⁶ The Report provides a very useful background to the legal and technical issues associated with developing EHR systems not only in Canada but in selected other countries too.

New Zealand

The Privacy Act 1993 sets out 12 information privacy principles²⁷ on collecting, using, keeping, disclosing, transferring, accessing and securing personal information.

Principles 1-4 govern the collection of personal information. This includes the reasons why personal information may be collected, where it may be collected from, and how it is collected. The general rule is that it should be collected from the individual concerned.

Principle 5 governs the way personal information is stored and safeguarded. It is designed to protect personal information from unauthorised use or disclosure.

Principle 6 gives individuals the right to access information about themselves and also sets out the situations where such access may be refused.

Principle 7 gives individuals the right to correct information about themselves and imposes a requirement on anyone who has disclosed inaccurate information to notify the recipients of that fact.

Principles 8-11 place restrictions on how people and organisations can use or disclose personal information. A general rule is that information obtained for one purpose cannot be used or disclosed for another purpose except in specified situations.

²⁶ Report prepared by University of Alberta, Health Law Institute and University of Victoria, School of Health Information Science (April 2005)

²⁷ Full information on the 12 privacy principles can be found at the New Zealand Privacy Commissioner's website www.privacy.org.nz

Principle 12 governs how “unique identifiers” can be used. Unique identifiers – such as bank customer numbers, driver’s licence and passport numbers – must not be assigned to individuals unless this is necessary for the organisation concerned to carry out its functions efficiently. The identifiers must be truly unique to each individual (except in some tax related circumstances), and the identity of individuals must be clearly established. No one is required to disclose their unique identifier unless it is for, or related to, one of the purposes for which the identifier was assigned. The Government is not allowed to give people one personal number to use in all their dealings with government agencies.

The Act also provides for codes of practice that can become legally binding. One such code is the *Health Information Privacy Code 1994*. The code sets specific rules for health sector agencies to ensure the protection of individuals’ personal information. In the health sector, the code takes the place of the Privacy Act’s information privacy principles, and deals with information collected, used, held and disclosed by health agencies.

In April 2007, the NZ Privacy Commissioner announced that she was seeking public submissions on proposed amendments to the Health Information Privacy Code 1994. The main proposed changes are to allow health practitioners to disclose, in certain specific circumstances, patients’ genetic information and to update the list of health agencies permitted to use National Health Index numbers to identify patients. As part of that process, the Commissioner published a paper entitled *Background Research Report on the National Health Index*²⁸ to provide information on the index and its associated Unique Identifier.

The New Zealand *Health Information Strategy*²⁹ was published in 2005 and like its Irish equivalent its focus is on maximizing information usage to help deliver a superior health system while recognizing the need to address privacy concerns.

Australia

As in other countries, Australia is also investing heavily in healthcare technologies and modern information systems. *HealthConnect* is the name of the overarching national change management strategy to develop the e-health agenda which includes Electronic Health Records and related Unique Health Identification systems. The strategy and implementation programmes are intended to facilitate the adoption of common standards by all e-health systems so that health information can be securely exchanged between health care providers such as doctors, specialists, pharmacists, hospitals and so on. The *HealthConnect* website³⁰ contains full details on the strategy and the importance it attaches to privacy issues. Its website also contains a full list of its publications including ones dealing with the legal, technical and privacy issues about unique identifiers and Electronic Health Records. Those papers reflect the Australian government’s view that

²⁸ Office of the Privacy Commissioner (April 2007)

²⁹ NZ Department of Health (2005)

³⁰ www.health.gov.au/internet/hconnect/publishing.nsf/Content/intro

voluntary participation (through an opt-in process) and consent are fundamental elements of the e-health agenda in Australia.

These issues are again to the fore in documentation and work of the body charged with implementing the strategy -*National E-Health Transition Authority*.³¹ Papers published by NEHTA include: *Privacy Blueprint - Unique Healthcare Identifiers v1.0*³², *NEHTA's Approach to Privacy v1.0*³³, *Shared Electronic Health Record Fact Sheet*³⁴ and the *Framework for Analysing, Planning and Implementing Identity Management within E-Health v1.0*³⁵. The *Privacy Blueprint* considered privacy issues mainly in the context of achieving the goals of EHRs and UHIs and paid particular attention to consent and notice, access, audit and secondary uses.

As in Canada, there is no specific Health Information Act at national level. The relevant Federal legislation is the Privacy Act 1988 and the Privacy (Amendment) (Private Sector) Act 2000. The 2000 Act applied the ten National Privacy Principles in the 1998 Act to health service providers in the private sector.

The 10 National Privacy Principles cover:

- Principle 1 - Collection
- Principle 2 - Use and disclosure
- Principle 3 - Data quality
- Principle 4 - Data security
- Principle 5 - Openness
- Principle 6 - Access and correction
- Principle 7 - Identifiers
- Principle 8 - Anonymity
- Principle 9 - Transborder data flows
- Principle 10 - Sensitive information

Section 6 of the Privacy Act defines 'health service' as an activity performed in relation to an individual:

- to assess, record, maintain or improve the individual's health;
- to diagnose the individual's illness or disability;
- to treat the individual's illness or disability or suspected illness or disability; or
- the dispensing of a prescription drug or medicinal preparation by a pharmacist.

Human genetic information was the topic of a joint federal inquiry by the Australian Law Reform Commission and the Australian Health Ethics Committee. The final report published in 2003-*Essentially Yours: The Protection of Human Genetic Information in*

³¹ www.nehta.gov.au

³² NEHTA (December 2006). The Report on Feedback was published in May 2007

³³ NEHTA (July 2006)

³⁴ NEHTA (August 2006)

³⁵ NEHTA (August 2007)

*Australia*³⁶ - contained a number of major recommendations one of which was that privacy laws should be harmonised and tailored to address the particular challenges of human genetic information, including extending protection to genetic samples, and acknowledging the familial dimension of genetic information. For example, doctors might be authorised to disclose confidential information to a genetic relative where it is necessary to avert a serious threat to an individual's life, health, or safety.

Guidelines on health related research have been developed by the (Australian) National Health and Medical Research Council (NHMRC) and approved by the Privacy Commissioner. The so-called *section 95 guidelines* seek to balance the protection of an individual's health information with the need for ethically approved research using individuals' health data without consent. The Guidelines allow Commonwealth agencies to disclose information (without consent) for the purposes of medical research, as long as the medical research is conducted in accordance with the terms of the guidelines. They prescribe procedures that Human Research Ethics Committees and researchers must adhere to in order for the disclosures of personal information from Commonwealth agencies to be lawful. The Guidelines can be viewed at www.nhmrc.gov.au/publications

State Legislation

Certain States and territories have enacted specific health information legislation.

New South Wales: (Health Records and Information Privacy Act 2003)

The Health Records and Information Privacy Act 2002 (HRIP Act) came into effect on 1 September 2004. It governs the handling of health information in the public sector, and it also seeks to regulate the handling of health information in the private sector in New South Wales. In December 2004 Privacy NSW developed four statutory guidelines under the HRIP Act. These guidelines³⁷ are legally binding documents that define the scope of particular exemptions in the health privacy principles in the following areas:

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

Victoria: (Health Records Act 2001)

The Victorian Health Records Act 2001 (Health Records Act) came into effect from 1 July 2002. This Act covers the handling of all personal information held by health service providers in the State public sector and also seeks to govern acts or practices in the Victorian private health sector. The Health Records Act contains a set of principles adapted from the National Privacy Principles.

³⁶ ALRC 1996

³⁷ Available on www.lawlink.nsw.gov.au/lawlink/privacynsw

Australian Capital Territory: (Health Records (Privacy and Access) Act 1997)

The Health Records (Privacy and Access) Act 1997 (Health Records Act) covers health records held in the public sector in the ACT and also seeks to apply to acts or practices in the private sector not covered by the Privacy Act. The Health Records Act contains privacy principles based on the federal legislation but modified to suit the requirements of health records.

Speeches –the speech by Andrew Hayne, Deputy Director, Policy, Office of the Privacy Commissioner on Privacy essentials for electronic health records³⁸ sets out the thinking of the office on Electronic Health Records the development of which are a key goal of the Australian Government HealthConnect programme.

United Kingdom

Legislation -In the United Kingdom, the following primary and secondary legislation is applicable to managing personal health information:

- Human Rights Act 1998 - This Act gave effect, in the UK, to the European Convention on Human Rights. It imposes a general requirement to protect the privacy of individuals and preserve the confidentiality of their health records and further required that the provisions of the UK Data Protection Acts must be interpreted in the light of the 1998 Act.
- Data Protection Acts 1984 & 1998 -As with Ireland, the first gave effect to the Council of Europe data protection Convention and the second implemented the EU data protection Directive.
- Health and Social Care Act 2001 -section 60 of this Act makes it lawful to disclose and use confidential patient information in specified circumstances where it is not practicable to satisfy the common law confidentiality obligations. This does not create new statutory gateways, so the processing must still be for a lawful function. However, it does mean that the consent obligation does not have to be met. Even where these powers apply however, the Data Protection Act 1998 also continues to apply. Section 60 was introduced primarily as a temporary measure which was intended to be transitional, allowing the NHS time to develop procedures for obtaining consent from patients or find ways of working with pseudonymised/anonymised information.³⁹
- Public Health (Control of Disease) Act 1984 and the Public Health (Infectious Diseases) Regulations 1988 –these provide for the reporting of infectious diseases.
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Data Protection (Subject Access Modification) (Health) Order 2000 - This Order provides for the partial exemption from the subject access provisions of the Data Protection Act 1998 but only to the extent to which the supply to the data subject

³⁸ Delivered to Consumer Health Forum: electronic health records consumer representatives meeting, 4 April 2006.

³⁹ As per the (English) Department of Health paper Best Research for Best Health: A New National Health Research Strategy-Consultation Questions (2005).

- of the information would be likely to cause serious harm to his or any other person's physical or mental health or condition.
- Health Service (Control of Patient Information) Regulations 2002 were the first regulations to be made under section 60 of this Health and Social Care Act, and support the operations of cancer registries and the Public Health Laboratory Services in respect of communicable diseases and other risks to public health.

Guides and Codes –the Department of Health and the National Health Service have provided guidance on the use of patient information. The main document is the *NHS Code of Practice on Patient Confidentiality*.⁴⁰ The Code's purpose is to provide guidance to the NHS and NHS-related organisations on patient information and confidentiality. It is a detailed document dealing with definitions, legal considerations, the importance of consent and a range of practical issues.

The issue of using personal health information for research purposes has attracted considerable discussion and diversity of opinion in the UK. An NHS study covering England & Wales, surveyed people's attitudes to consent and confidentiality of patient information –*Share with Care: People's Views on Consent & Confidentiality of Patient Information*– reported that people gave much higher priority to spending NHS money on patient care than on schemes to enable better information-sharing, to protect their confidentiality or to give them access to their own health records.

The British Information Commissioner (who has responsibility for data protection) also published a detailed guidance on the data protection obligations applicable to using health information –*Use and Disclosure of Health Data: Guidance on the Application of the data protection Act 1998*.⁴¹ A theme that the Commissioner was keen to emphasise in his guide was the need for a proper understanding in handling health information of the relationship between the application of the data protection principles in the 1998 Act and the common law duty of confidentiality.

European

At European level, and in individual European countries, there is considerable law and material on privacy, confidentiality and security of health information. One major data protection body operating at EU level is the *EU Article 29 Working Party*. The Working Party is composed of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission.⁴² It is an important platform for EU wide co-operation on data protection.

In February 2007, the Working Party adopted a *Working Document on the Processing of Personal Data in Electronic Health Records*.⁴³ The Document provides guidance on the interpretation of the applicable data protection framework for EHR systems and explains some of the general legal principles that should underpin the development of these

⁴⁰ Department of Health (7 November 2003)

⁴¹ Office of the (British) Information Commissioner (2002)

⁴² The EU Commission provides the WP Secretariat.

⁴³ WP131: Available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf.

systems. It also outlines the legal, technical and other safeguards that should be put in place.

In June of this year, the Working Party adopted an *Opinion on the Definition of Personal Data* (Opinion 4/2007). This Opinion is intended to provide guidance on a common understanding of the concept of “personal data” as defined in Directive 95/46/EC.⁴⁴

European Perspective on Confidentiality

The importance attached throughout Europe to confidentiality in the medical area is not confined to common law countries, like Ireland and the UK. The EU funded EuroSOCAP Project⁴⁵ which was concerned with European standards on confidentiality and privacy in healthcare stated in its 2006 report (*European Standards on Confidentiality and Privacy in Healthcare*):

“the importance of maintaining confidentiality in the practice of healthcare has been recognised continuously over the two and a half millennia since the composition of the Hippocratic Oath. Medical confidentiality has been consistently upheld as a core value of European healthcare through profound cultural, technological, political, social and economic changes. It remains a core value to this day and in modern Europe finds expression in three key principles of healthcare confidentiality.”

The EuroSOCAP Project identified the following shared European legal principles on confidentiality:

- (a) there is a prima facie obligation to maintain confidentiality when information has been imparted to a professional within a confidentiality relationship;
- (b) this obligation to maintain confidentiality can be discharged when the subject of the confidence affords appropriate consent to the disclosure of the information; and
- (c) in providing a justification for the non-consensual disclosure of confidential information healthcare professionals should have particular regard to issues such as:
 - (i) the necessity of any particular disclosure;
 - (ii) the proportionality of any particular disclosure;
 - (iii) the risks attendant upon any particular disclosure; and
 - (iv) the existence of identifiable risks of serious harm to identifiable third parties arising from nondisclosure.

⁴⁴ The full text of the opinion is available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

⁴⁵ The project was made up of 20 members –clinicians, therapists, legal experts and ethicists- from 11 EU States

The thrust of the EuroSACAP Report was that the nature of the relationship between healthcare professional and patient and respect for the patient's autonomy constitute powerful reasons for protection of personal information. Taken together they strengthen the case for the non-use or non-disclosure of private information about a patient. There are also other justifications. For example, one reason for respecting confidences in healthcare is that doing so enables patients to disclose sensitive information that the healthcare professional needs to carry out treatment. Without an assurance that confidentiality will be maintained, patients might be less willing to disclose information, resulting in negative effects for their health, for public health and for healthcare practice. The patient's right to self determination in matters of information sharing could also be justified on other grounds. These include the view that the patient is in the best position to understand and therefore protect his or her own interests, and that there is an intrinsic value in people deciding about and taking responsibility for their own lives. This confidentiality obligation is also consistent with the patient's right to self-determination in various other healthcare matters, such as the right to choose to refuse surgery.

The Report also made the point that "ethical standards of healthcare professional confidentiality are not reducible to data protection standards, although they operate in conjunction with them."⁴⁶

The Report concluded that:

- *individuals have a fundamental right to the privacy and confidentiality of their health information.*
- *individuals have a right to control access to and disclosure of their own health information by giving, withholding or withdrawing consent.*
- *for any unauthorized disclosure of confidential information healthcare professionals should have regard to its necessity, proportionality and attendant risks.*

⁴⁶ EuroSOCAP Report, page 4.

Appendix: Health Information Principles

Obtaining, Organising and Holding Personal Health Information

Personal Health Information should be:

- obtained and processed fairly which means that, as far as possible, it should be obtained from the patient with his or her explicit consent and, irrespective of whom it is collected from, the individual providing it should be aware of the purposes for which the information may be used and the persons or categories of persons to whom it may be disclosed;
- relevant, accurate and up-to-date as well as intelligible to others who may require it for diagnosis and treatment purposes;
- adequate but not excessive which requires a consideration by the general practitioner involved of the information and its intended uses. This would mean that records should include: symptoms voiced by the patient; tests undertaken; facts, analysis and opinions presented to the patient; correspondence from the patient or other parties; the identification of problems that have arisen and the action taken to rectify them, evidence of the care planned, decisions made, care delivered and information shared;
- devoid of irrelevant, prejudicial, derogatory, malicious, vexatious information or comment;
- organized in a manner that minimises the potential for the personal health information of one individual being confused with another; documented, dated and well organised for efficient retrieval, comprehensible and legible which is especially important if some other health professional is required to use them in an emergency situation,
- held no longer than is necessary which may, as appropriate, depending on circumstances be indefinitely⁴⁷;
- purpose specific which means that it must be used only for the lawful purposes for which it was collected.

Security of Personal Health Information

Personal health information should be held securely, safely and consistently which requires the taking of appropriate security measures against unauthorised access, alteration, disclosure or destruction. These include: physical, technical and organisational measures and especially, where information is shared, audit trails.

Practices that may lead to breaches of security include:

⁴⁷ It is accepted medical practice that individual patient medical records be retained for a *minimum* of eight years from the date of last contact or for any period prescribed by law. (In the case of children's records, the period of eight years generally begins from the time they reach the age of majority). In other cases, healthcare professionals or agencies holding personal health information may decide that it is in the patient's, and their own, best interests that it should be retained indefinitely.

- ◆ Leaving medical notes unattended at a public counter.
- ◆ Not disposing of health records in a secure manner.
- ◆ Inadequate controls regarding which staff can access health information – this might include inadequate password control on a database.
- ◆ Storing sensitive data on a laptop computer that is taken off-site and not stored securely.

Integrity is concerned with preserving the consistency and the accuracy of data; protecting against both malicious and accidental interference, even by authorised users. It applies both to correctness of data and to mechanisms that help to ensure the correctness of data.

Using, Disclosing and Transferring Personal Health Information

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

- for the purpose for which it was collected; or
- for another directly-related purpose that is within the reasonable expectations of the patient at the time he or she provided the information.

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

- the patient concerned has consented to the use or disclosure; or
- the medical practitioner reasonably believes the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's life, health or safety, or a serious threat to public health or public safety; or
- the use or disclosure is required or authorised by law (e.g. statutory duties to notify certain infectious diseases or suspected child abuse, or compliance with a subpoena or court order); or
- the information concerns a patient who is incapable of giving consent, and is disclosed to a person responsible for the patient to enable appropriate care or treatment to be provided to the patient.

Any disclosure should be limited to that which is either authorised or required in order to achieve the desired objective.

Personal health information can be transferred to an individual or organisation outside the European Economic Area only if:

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

The general principle governing the use, disclosure or transfer of all personal health information is that the patient must understand what the healthcare professional proposes

to do with the information and must agree with this proposed use. Only in certain very limited circumstances is it lawful to use, disclose or transfer personal health information without the consent of the patient.

Patient Consent To Collecting Information

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

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

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

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

Patient Access to Personal Health Information

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

The general rule is that patients have a right to have access to their personal health information irrespective of the form in which it is kept.

Where a patient requests an alteration or correction to their personal health information, healthcare professionals should note details of the request on the medical record and indicate whether they agree that the request for alteration or correction is appropriate.

Healthcare professional can refuse patients access to their personal health information only if:

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

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