

**DISCUSSION PAPER ON
PROPOSED HEALTH INFORMATION BILL**

JUNE 2008

CONTENTS

THE ACCOMPANYING AUDIT OF KEY INTERNATIONAL INSTRUMENTS, NATIONAL LAW AND GUIDELINES RELATING TO HEALTH INFORMATION FOR IRELAND AND SELECTED OTHER COUNTRIES HAS BEEN PREPARED TO COMPLEMENT THE INFORMATION IN THIS DOCUMENT AND SHOULD BE CONSULTED WHERE THE READER IS INTERESTED IN FINDING OUT MORE ABOUT THE SUBJECT AREA.

	Page
PURPOSE OF THE DISCUSSION PAPER	2
EXECUTIVE SUMMARY	4
PART 1: OBJECTIVES OF THE HEALTH INFORMATION BILL	7
PART 2: IMPORTANT INFORMATION CONCEPTS	16
PART 3: THE EXISTING REGULATORY ENVIRONMENT	19
Appendix 1: Electronic Health Records	30
Appendix 2: Unique Health Identifiers	37
Appendix 3: Population Registers	45
Appendix 4: Use of Information for Medical Research	47

PURPOSE OF THIS DISCUSSION PAPER

The purpose of this Discussion Paper is to facilitate the preparation of the Health Information Bill by ensuring an informed consideration of the relevant issues. The Bill is about the better use of personal health information –whether in manual or electronic form- for improved patient care and safety and the achievement of other health service objectives.

In the Information Society, there is an increasing awareness of the value of personal information. At the same time, developments in information technology have increased the threat to the privacy of the individual. However, the fundamental issues associated with protecting personal health information –that is privacy, confidentiality, consent and security- pre-date the information technology revolution. Modern technology has, for the most part, simply brought the issues into sharper focus.

Personal health information, in whatever form, is sensitive. It is regarded by patients as private and the expectation is that it will be kept confidential and secure. It is collected, used and disclosed primarily for the treatment and care of the individual to whom it relates. It is widely recognized, however, that it can have other positive uses that would benefit the health system as a whole in facilitating better planning, management and delivery of services. It can also be important in facilitating certain types of research projects that require the identification of the potential participants in the studies.

The objective of the current Health Reform Programme is to deliver better patient care and safety. This means using information –in manual and electronic form- more effectively than previously to improve healthcare outcomes while ensuring that an individual's control over his or her personal health information is appropriately respected. This requires an examination of how information is used, the areas where it could be better used and the safeguards needed to ensure appropriate protection.

The experience from other countries indicates that the health reform process, increasing emphasis on information management and eHealth initiatives are likely to impact on long-established principles of patient privacy, common law traditions of confidentiality as well as longstanding professional and ethical codes on using and safeguarding personal health information.

To date, there has been no real public debate around the issue in Ireland. However, in the context of preparing legislation in the form of a Health Information Bill, it is essential that the relevant issues are clearly identified, considered and addressed.

Accordingly, the structure of this Discussion Paper is to set out the policy objectives that should drive the proposed Health Information Bill (Part 1). In doing so, it will be necessary to have regard to key information concepts such as privacy, confidentiality, consent, security and integrity (Part 2) and to the current regulatory environment for collecting, using, retaining and disclosing personal health information (Parts 3). The Appendices provides details on certain major areas, such as the development of Electronic Health Records, including an overview of how they are being dealt with in

certain other countries. The accompanying Audit Document looks in greater detail at applicable international principles and national laws.

KEY ISSUES FOR CONSIDERATION

The purpose of this Discussion Paper is to ensure that there is informed consideration on the relevant issues to be addressed in the Health Information Bill. National and international experience suggests that the key issues relate to the following areas.

- 1. What are the benefits to patient care and safety which should be the objectives of any legislation? (see Part 1)**
- 2. What is the balance to be struck between the right of individuals to control their healthcare information and the needs of those managing healthcare systems, providing healthcare services and undertaking medical research (including the role of Research Ethics Committees) to have limited and controlled access, without individual consent, to such information for legitimate purposes? (See Parts 2 and 3 and Appendices)**
- 3. What rules should accompany the introduction of a Unique Health Identifier for both patients and healthcare providers? In particular, what factors should influence the regulation of the collection, use, disclosure and linkage of such an identifier? (See Appendix 2)**
- 4. What legal issues need to be considered in establishing a National Electronic Health Records system: especially as regards an individual's choice to participate or not and his or her control over the extent of any participation? (See Appendix 1)**
- 5. What principles should guide the development and regulation of National Health Population Registers, such as the National Cancer Registry, and the instances in which reporting to such registers should be mandatory? (See Appendix 3)**
- 6. What needs to be done to provide consistency and clarity in and between legislation, other legal rules and professional ethical codes in the treatment of personal health information having regards to considerations of privacy, confidentiality, consent and security? (See Parts 2 and 3)**
- 7. Is there a need for a comprehensive definition of personal health information and, if so, what should it encompass? (See Parts 2 and 3)**
- 8. To what extent do certain categories of personal health information -for example, mental health information and information on children and deceased individuals - require special rules on collecting, keeping, using, disclosing and accessing? (See Parts 2 and 3)**
- 9. Should the Health Information Bill be a comprehensive piece of legislation dealing with all the relevant issues or should it build on the legislative framework (data protection and freedom of information) that is already there and working well? (See Part 1)**

EXECUTIVE SUMMARY

Purpose of the Health Information Bill

This Discussion Paper is concerned with the proposed Health Information Bill which is a major element in the Healthcare Reform Programme. The main purposes of the Bill are:

- to establish a legislative framework to enable information –in whatever form- to be used to best effect to enhance medical care and patient safety,
- to facilitate the greater use of information technologies for better delivery of patient services, and
- to underpin an effective information governance structure for the health system generally.

Structure of the Discussion Paper

The objective of the Discussion Paper (and the accompanying Audit of Key International Instruments, National Law and Guidelines relating to Health Information for Ireland and Selected Other Countries) is to facilitate an informed discussion on the above. Accordingly, the Paper is structured in the following way. Part 1 sets out the objectives of the Health Information Bill. Part 2 then examines key information issues. This is followed by an outline of the current regulatory framework applicable to information in the Irish health system (Part 3). The Appendices provide detail information on certain areas: namely, Electronic Health Records, Unique Health Identification, Population Health Registers and using patient identifiable information for research.

Part 1: Objectives of the Health Information Bill

Better patient care is dependent on using information in both manual and electronic formats more efficiently and effectively. Information and communications technologies can make a major contribution to enhancing the quality, quantity and timeliness of information available to clinicians and health service managers. At present, the ability of healthcare professionals to access up-to-date health information about a patient, whenever and wherever necessary, is limited and fragmented.

The Health Information Bill will give effect to a number of key policy objectives. In particular, it will ensure that there is a sound legislative base for the use and sharing of information throughout the health system so as to provide best patient care and safety and make certain that health information can flow between the public and private health sectors in line with patient care requirements. It will also ensure that new technologies with major potential for improved care and safety, such as Electronic Health Record systems, have a secure legislative base to facilitate their development.

Part 2 Key Information Issues

Personal health information is sensitive and patients expect their medical data to be safeguarded especially from uses or disclosures which they would be unaware of or disagree with. The discussion on collecting, using, keeping, storing and disclosing

personal health information is, therefore, about ensuring its privacy (the right of an individual to control how his or her information is used), confidentiality (the obligation on the person holding the information not to disclose it without consent), security (the physical and other protections in place to prevent unauthorized access) and integrity (measures applied to ensure the quality of the data).

A major debate, internationally, centres on the need to balance potentially competing (individual) rights and (societal) needs. In the health sector, this is about the rights of the patient to determine who has access to his or her medical records and the needs of the health service to use patient information for a range of management and research purposes that stand to benefit both the individual patient directly and society generally, through better service planning and healthcare innovations.

The extent to which patient consent should determine the use and disclosure of personal health information is a critical matter. For that reason, this Part also looks at the nature of consent, the forms it may take and the qualities that need to be present so that it can be regarded as valid. Exceptions, in existing law, to the consent principle are also considered.

Part 3: The Present Regulatory Structure

The present regulatory framework for the use of health information is shaped by national and international sources.

- *international instruments and agreement,*
- *international data protection initiatives,*
- *European Union initiatives,*
- *national law,*
- *professional ethical codes,*
- *decisions and guidance of supervisory authorities and Courts*

The **Appendices** deal with:

-Providing the legal framework for the development of Electronic Health Records (Appendix 1);

-Establishing the legal principles underpinning the introduction of a Unique Health Identifier (Appendix 2);

-Setting out the legal basis for creating Population Health Registers (Appendix 3);

-Clarifying the use and disclosure of information for health research purposes (Appendix 4).

PART 1: OBJECTIVES OF THE HEALTH INFORMATION BILL

Legislation –in the form of a Health Information Bill- has a significant role to play in the health information management process by both removing existing obstacles to the flow of information as well as facilitating new technologies that help patient treatment. It will underpin a national and system wide information governance framework for the modern Irish health service. That framework is an essential starting point for the delivery of the benefits above.

1.1 INFORMATION AND OUR HEALTH SYSTEM

Our health care system depends on, and in effect runs on, information. For the most part, that information is created through interactions by individuals with healthcare professionals across a range of healthcare settings including general practice, acute hospital care, out patient departments, accident and emergency units, high street pharmacies and so forth. Some of that information is still kept in manual format but increasingly it is held electronically. The Health Information Bill is concerned with personal health information in whatever form it is collected, kept, used and disclosed.

The quality management of information is indispensable to the quality of healthcare.

The case for eHealth by Denise Silber (2003)¹

It is clear that high-quality information should be at the centre of all decisions concerning health especially individual patient safety and care and also, more generally, the planning and management of health services nationally and locally.

The ability of healthcare professionals to access up-to-date health information about an individual whenever and wherever necessary is, currently, limited and fragmented. This is due to the shortcomings of paper-based records, or, where computerised clinical records are available, the inability of these records to be shared across different computer software systems. This results in individual points of care becoming ‘islands of information’ at the very time when proper clinical care requires otherwise.

This lack of timely access to relevant information increases the risk of individuals not receiving appropriate care. It can also result in an accumulation of inefficiencies in the health system, such as the unnecessary repetition of diagnostic tests. Achieving better healthcare outcomes, whether for particular patients or the health services generally, through better decision-making involves a commitment to bringing accurate, up-to-date, relevant and timely information to the points in the health system where it is required.

International experience shows that the proper use of quality based information systems and modern communications technology (ICT) in Irish healthcare -sometimes referred to as e-health solutions- has the potential to make a major contribution² to:

¹ Presented at the EU Commission’s First High Level Conference on eHealth (May 2003)

² The article “Health Informatics: Managing Information to Deliver Value” (by Ball, Douglas and Lillis (Medinfo 2001: 10 (pt 1) 305-8) provides a wider-ranging review of the benefits of eHealth

-improved patient safety, there is growing evidence that the use of information and technology improves safety, quality, and continuity of care. There is also consistent evidence that errors can be reduced by the appropriate use of ICT particularly in drug prescribing by flagging

allergies and contra-indications and in the dispensing and administration of medications,

Evidence suggests that in advanced healthcare systems medical errors are killing more people each year than breast cancer, AIDS or motor vehicle accidents together. About one in ten patients admitted to a hospital is unintentionally harmed. These stark figures illustrate the current shortcomings in the domain of patient safety. ICT can make a vital contribution in reducing errors, thereby saving lives and enhancing efficiency – and improving the quality of care for European citizens.

EU Study Impact of ICT on Patient Safety and Risk Management (eHealth for Safety)³ (2007)

-more evidenced based care and seamless integrated care across all health care sectors and environments because information will follow the patient through the system and be available where it is needed and when it is needed,

Sharing information appropriately across different care delivery settings is very important for ensuring safe and high-quality care for patients. Healthcare must be focused on improving the co-ordination between different areas of the sector in order to improve overall outcomes or to create efficiencies by automating simple tasks. For example, sharing information between providers improves the quality of care by reducing unnecessary repeat tests and by eliminating the need to repeat information to multiple providers.

New Zealand Health Information Strategy(2005)⁴

-greater financial efficiency in healthcare services, studies indicate that ICT has the potential to reduce inefficient use of resources by cutting duplication, excessive paper handling, administrative activity etc,

-empowerment of patients and other healthcare consumers by opening up health related knowledge bases to assist choice thereby facilitating a new information based relationship between patients and healthcare professionals and health agencies,

³ Available at http://ec.europa.eu/information_society/activities/health/studies/studies05-06/patient_safety/index_en.htm

⁴ Health Information Strategy for New Zealand: Ministry of Health (August 2005)

-improved planning, management and delivery of health services and health projects through better information management, enhanced business planning and control and greater risk management,

-better research and disease management outcomes which benefit both individuals and society due to total population studies rather than limited sample ones,

-establishing new data collections and data sets that will help identify and manage the specific health needs of defined population groups across different care settings,

-mitigating public health and other population threats by improving our ability to detect and respond quickly, for example, to disease outbreaks,

-extending the scope of healthcare beyond its current boundaries through: for example, telemedicine which has particular relevance for rural and island communities,

-more accessible continuing education for healthcare professionals through online training models, and

-enhancing the privacy, confidentiality, integrity and security of patient information through the computerized tracking and auditing of access to patient records.

However, the potential benefits of e-health can only be met within a framework which includes the following elements:-

-the development of a standards based approach to information and technology that ensures proper building blocks are put in place that can be evolved to meet changing needs,

extending the collection of information into those health areas where we currently lack vital information to support decision making and targeting of services,

- promoting an awareness throughout the health system and all levels, including the patient, that sees information as a valuable asset linked directly to better outcomes for individual patients and society generally,

-the implementation of information and technology solutions which are capable of supporting the objectives of health information policy in a clearly defined, efficient and cost effective manner,

-involving all stakeholders in a genuine consultative process to make certain that information systems are developed to meet their needs,

-emphasising a value for money approach to information systems development,

-enshrining the need for ongoing review of information systems to ensure they remain useful over time.

Fully realizing these elements requires cultural change throughout our health system to embrace the role information can play in sustaining an environment that adapts quickly to evolving needs, pressures and resources. The establishment of the new institutional framework for the Irish health system and the creation of a robust information structure will work best where information is placed at the centre of decision-making.

1.2 HEALTH INFORMATION AND THE HEALTH REFORM PROGRAMME⁵

Legislation reflects values in society. The values context which underpins the Health Information Bill is grounded on the goals and philosophy of the wider health reform programme. That programme is concerned with creating a modern patient-centred healthcare system in Ireland and includes the strategic development of health information so as to ensure that the highest levels of health and social well-being are achieved for individuals and the whole population.

1.2.1 Institutional Reform

Recent years have seen major institutional reform⁶ in the Irish health system with the establishment of the Health Service Executive⁷, the creation of the Health Information and Quality Authority⁸ and the adoption of a stronger policy and performance evaluation role by the Department of Health & Children. The Health Information Bill is an important part of the reform programme because better information governance is essential for the programme to succeed.

1.2.2 The Information Dimension of the Reform Process

Health Information: A National Strategy (the National Health Information Strategy) (2004) recommended a series of actions both to rectify present deficiencies in health information systems and to put in place the frameworks to ensure the optimal development and utilisation of health information.⁹

Action 116 of the National Health Information Strategy called for a sustained programme of investment in the development of national health information systems, while Action 117 asserted that information and communications technology will be fully exploited in service delivery. Chapter 10 of the current National Development Plan relates to the Health Information and Communications Technology Investment Sub-Programme and provides that capital funding of €490m will be provided under this heading in the Health area under the Plan. It states

⁵ Part 3 of the accompanying Audit document contains further details on the strategies and reports underpinning the reform process.

⁶ The previous major re-organisation of the Irish Health System took place in the early 1970s.

⁷ Established by the Health Act 2004.

⁸ Created by the Health Act 2007.

⁹ In recent years, a number of countries have produced Health Information Strategies, for example, *Health Information Strategy for New Zealand*, NZ Ministry of Health (August 2005).

“...ICT enabled health care is essential to ensuring that care is delivered in a safe and more efficient manner by providing complete, accurate, and timely information at the point of care, whether within the hospital setting, in the community, or in the home.”¹⁰

The Information Strategy also outlined the problems/deficiencies arising under the present legislative and regulatory structures. The Health Act 2007 addressed some of the information issues: in particular, by providing for the establishment of the Health Information and Quality Authority and giving it information functions.

The Information Strategy regarded it as particularly important that proper information governance arrangements should exist on a system wide basis throughout the Irish health system. This would provide “a set of rules to ensure full and proper use of information while fully protecting the privacy of the individual”.¹¹ It saw the Health Information Bill as helping to create a new and rigorous information governance framework.¹²

1.3 POLICY OBJECTIVES OF THE HEALTH INFORMATION BILL

Following on from the above, the central policy objective of the Health Information Bill is to support the creation of an effective system-wide health information governance framework that is focussed on patient care and safety. The associated major challenge is to build public confidence in this process through legislative principles that are workable, transparent and widely supported.

Specifically, the goals of the proposed Health Information Bill should be to:

- ensure that there is a sound legislative base for the use of information throughout the health system so as to provide best patient care and safety;
- ensure that health information can flow between the public and private health sectors in line with patient care requirements;
- ensuring that individuals can access their health information (subject access rights) without compromising public policy on matters such as adoption related records or third party provision of information (in confidence and in good faith);
- provide that healthcare professionals will be required to forward, on request, a full copy of the medical records of their patients to another healthcare professional where the patient so requests and to similarly deal with the situation where a healthcare professional in either the public or private sector retires or resigns from practice;

¹⁰ National Development Plan 2007-2013: Transforming Ireland (Chap 10)

¹¹ The need for such a framework and Bill had already been expressly referred to in the National Health Strategy (2001).

¹² Action 17, pages 74-75

- facilitate, in a transparent and accountable manner, the development of modern information systems and technologies that benefit the patient, such as the Electronic Health Record;
- allow for the introduction of a Unique Health Identifier (that would have regard to any other relevant work being done in developing identifiers for use in the public services);
- facilitate the establishment of national population registries (similar to the National Cancer Registry);
- define “personal health information” in a way that is relevant to the modern Irish health system and address particular issues relating to genetic information;
- protect the privacy, confidentiality, security and integrity of personal health information and ensure that these principles apply explicitly to all persons (and not just clinicians) who have a legitimate reason, in certain situations, to be involved with or access such information: for example, medical students, healthcare administrative personnel, software and hardware vendors who supply and maintain health information systems;
- protect the traditional trust relationship between healthcare professionals and patients by ensuring clarity for clinicians and others in relation to what information they have discretion to disclose and the circumstances in which they are required to disclose;
- provide special rules, where appropriate, to deal with particular categories of personal health information, for example, Mental Health Records; to ensure that the rights of the individual concerned are fully supported with due regard to the legitimate interests of others;¹³
- safeguard the rights of children in relation to their personal health information and, at the same time, vindicate the right of parents to have access to such information as is required to act in their children’s best interest;
- enhance consistency, where necessary, between the Data Protection and Freedom of Information regimes (for example, in the treatment of records of deceased individuals) and providing a reference point for the updating of professional ethical codes in the health sector based on uniform principles;
- facilitate the development of best practice codes (for different sectors of the health system which could deal with issues applicable to that particular sector only);

¹³ The Information Commissioner has stated that family members are often concerned that they might be identified, from the patient's records, as having given information to a doctor or hospital in relation to the patient. Generally, the current FOI Act protects the family members in these instances and it will be important to ensure that necessary protection continues to be possible.

- establish a framework that provides clarity to all involved on the obtaining, use, retention and disclosure of identifiable personal health information (including genetic data) for management (for example, clinical audit) and research purposes (including the role of Research Ethics Committees) in situations other than where the informed consent of the individual is given and address concerns, in the research community, about the current absence of a structure for ethical approval of health and social service research projects;
- provide a clear and enforceable framework for better record management practices throughout the health system.

1.4 LEGISLATIVE OPTIONS

The preparation of the Health Information Bill will have to have regard to the Constitution, international instruments (such as the European Convention on Human Rights), EU Data Protection Directives, existing data protection and FOI legislation, the law of confidence and established ethical codes.

The fundamental question is whether the proposed Bill should seek to create a wholly new and stand alone structure for all matters relating to personal health information (*Option 1*, below) or should build on what is already there and working well (*Option 2*, below).

Option 1: to create a stand alone health information regulatory structure.

Option 2: to build on what is already there and working.

Option 1- The first would be to separate, to the greatest extent possible, the regulation of health information from existing data protection and FOI legislation. This would mean a Bill that attempted to address every issue relating to the collection, use, disclosure etc of personal health information. It would, in effect, create a completely new regulatory environment for the management of health information which would require its own separate supervisory authority.

Such an approach would have the advantage of being a single comprehensive piece of legislation relevant to the health sector.

However, it would also have a number of disadvantages. First, the health sector does not exist in isolation from other sectors of society and it is frequently not easy or sometimes appropriate to view health information as wholly distinct from other personal information kept on individuals. This could give rise to confusing and conflicting rules applying. Secondly, removing the health sector from the remit of FOI or DP legislation might be viewed as setting an unacceptable policy precedent. Third, there would be legitimate arguments that any new legislation should not adversely affect anything that is already in place and working well. Fourth, the more that is changed the greater the potential compliance and other costs will be without any guarantee of equivalent corresponding benefit to patients and others. Fifth, the more wide-ranging any Bill is the greater the likelihood that consultations with stakeholders will be protracted and complicated thus delaying any action required.

Option 2- There is an alternative approach that is very much focused on the specific areas identified as needing attention. It starts from the perspective of continuing to use what is already there and building on it only to the extent necessary to facilitate the appropriate flow of information through the health system for better patient care.

The benefits of the above approach are that it is targeted. It avoids duplication and re-inventing the wheel. Rather than creating a whole new information management superstructure, it will add to what is already familiar. It would, for example, address the need for a legal basis for the EHR and UHI and facilitate necessary research which might otherwise fail because of problems obtaining consent from everyone involved and at the same time ensures that privacy concerns are assured. Importantly, it would not disturb areas which are working well.

1.6 AN EXAMPLE: THE NATIONAL HEALTHLINK PROJECT

The National Healthlink Project¹⁴ is an Irish e-health project that has won several awards, including at EU level. It is an electronic communications project that transmits test results between a hospital and a patient's general practitioner. Test results are crucial to the proper diagnosis and care of patients. The faster they become available, the better for the patient. Healthlink provides that speed and has been designed so that results can be integrated directly into the patient's individual record in the GP surgery thereby ensuring ready accessibility as part of a fuller record.

There are¹⁵ 529 general practices (working out at 1176 General Practitioners) registered with Healthlink with 18 acute hospitals and other health agencies involved.

The message types currently online are:

- Laboratory Results
- Radiology Result
- Death Notifications
- Discharge Notifications
- Discharge Summaries
- A & E Attendance Notification
- Waiting List Updates
- OPD Appointment Updates

As well as patient benefits, there are administrative and clinical advantages for the participating General Practices and hospital in terms of efficiency; including

- reduction in phone calls to hospital lab - time saving
- reduction in administration (& admin costs)
- reduction in clerical errors from manually entering data
- integration of the test result into the GP's Practice Management System.

¹⁴ www.healthlink.ie

¹⁵ 1 October 2007

PART 2: IMPORTANT INFORMATION CONCEPTS

2.1 KEY TERMS

Throughout this Discussion Paper the terms privacy, security, confidentiality and consent will be used frequently. It is important, therefore, to appreciate that while they each relate to protecting personal information they cover different aspects of such protection.

The key terms are:

**PRIVACY,
CONFIDENTIALITY,
SECURITY,
INTEGRITY,
CONSENT**

2.1 PRIVACY, CONFIDENTIALITY, SECURITY AND INTEGRITY

The terms “privacy”, “security” and “confidentiality” are sometimes used interchangeably but, while related, they are not the same. “Privacy” is the right to control how our information is obtained, used and disclosed etc. It is “privacy” that drives the duty of “confidentiality” and the responsibility for “security”. Accordingly, while it is very important that health information should be kept securely, it does not, of itself, guarantee privacy unless it is the individual concerned who decides the purposes for which it can be used or the persons to whom it can be disclosed.

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. (These are discussed in greater detail in Part 3 of this Paper).

Security refers to measures taken to safeguard personal information from unauthorized access, use or disclosure. Some distinguish between data security and system security. Data security results from measures that effectively protect data and computer programs from threats such as unauthorized access and disclosure; impermissible alteration; unauthorized copying; theft; etc. In contrast, system security refers to the sum of all measures in place – including, personnel policies, practices for monitoring compliance, and so on – that are aimed at protecting personal information.

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.

2.2 CONSENT

CONSENT

Consent must always be informed to be valid. It can be either:

Implicit/ implied, or

Explicit/ express

Informed consent requires adequate and appropriate information to be provided and capacity and competency to be present in the individual concerned.

2.2.1 Informed Consent

Consent always has to be informed¹⁶ to be valid. While there is no single definition of consent in Irish law, the EU Data Protection Directive (95/46/EC) defines it as:

“... any freely given specific and informed indication of his [or her] wishes by which the data subject signifies his [or her] agreement to personal data relating to him [or her] being processed.”

2.2.2 Elements of Informed Consent

It is accepted that certain elements must be present, if the consent is to be regarded as valid, including:

- awareness (through the provision of suitable information) and understanding (capacity and competence) of the nature and extent of the processing, especially in terms of intended and likely uses and disclosures of the information involved;
- awareness of option(s) to prevent such processing either in whole or in relation to any particular aspect;
- the existence of a mechanism to enable the option of withholding consent to be effective; and
- absence of coercion.

2.2.3 Implicit Consent

Consent can be implicit (implied) or explicit (express). Where consent can validly be inferred, implied consent is not a lesser form of consent than express consent.¹⁷

However, express consent allows for clearer verification.

On implicit consent, Jennifer Stoddart, the Privacy Commissioner for Canada, stated that:

“... [her] office recognises ... the principle of implied consent for information to flow freely within the ‘circle of care’. The definitions around the ‘circle of care’ relate to the care and treatment of the patient and healthcare services for

¹⁶ Consent can never be valid, if prohibited by law.

¹⁷ For example, the UK Information Commissioner stated “It is a mistake to assume that implied consent is a less valid form of consent than express. Both must be equally informed and both must express the wishes of the patient.” (Information Commissioner (UK) (2002), p.14).

the therapeutic benefit of the patient. This would include laboratory work and professional case consultation with other healthcare providers.”¹⁸

Implied consent, therefore, covers the sharing of information within a primary care team, or beyond to secondary or tertiary care providers, where such sharing is related only to the care of the patient concerned. Implied consent normally would also cover such secondary purposes as business and administrative uses that arise from, and are directly related to, the treatment and care of the patient. In these situations, the amount of personal information used and disclosed must be kept to the minimum necessary. It would not cover anything outside the above, such as the communication of information for teaching or third-party research.

2.2.4 Explicit Consent

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

2.2.5 Issues with Explicit Consent

While explicit consent for all healthcare purposes would resolve doubts about the uses and disclosures of personal health information, such an approach raises questions as to whether it may:

- ◆ be too expensive and bureaucratic,
- ◆ not possible to reach whole sample populations for research,
- ◆ disruptive of healthcare services,
- ◆ lead to the diversion of resources from the primary purpose of healthcare.

2.2.6 Obtaining, Withholding & Withdrawing Consent

As a general rule, consent should be obtained at the beginning of any healthcare relationship. Consent is not required at the time of every subsequent visit /contact, but only when there is a material change in the anticipated use or disclosure of the patient’s information. Patients can refuse to provide certain personal health information or may withhold consent for particular uses or disclosure of that information. Where patients are competent to make such a choice and where the consequences of the choice have been fully explained, the decision should be respected.

2.2.7 Expectations & Awareness

It is worth explaining that expectation is more than awareness – telling someone about proposed secondary uses or disclosures may not necessarily create a reasonable expectation. A healthcare data controller needs to consider the kind of person they are talking to, what their understanding is likely to be and therefore what they may reasonably expect. This means having regard to factors such as the individual’s age, sex or cultural, linguistic and socio-economic background. If an individual expresses negative views, when made aware of a proposed secondary use or disclosure of their

¹⁸ This speech can be found in the Resource sub-menu of the Canadian Privacy Commissioner’s website, <http://www.privcom.gc.ca>.

personal information, this would indicate ordinarily that they would not reasonably expect that use.

2.2.8 Silence as Consent and Small Print

A major practical consideration is whether so-called passive consent mechanisms are acceptable as a means of obtaining valid consent. Such an approach arises when a data controller communicates with a data subject, advising that he intends to use the data subject's information in some way unless the individual indicates otherwise. In his 1997 *Annual Report*, the then Data Protection Commissioner rejected such an approach. In the same Annual Report, the issue of consent through small print was considered and also rejected.

2.2.9 Exceptions to consent

There are exceptions to the consent principle in both law and under medical ethics. These include:

Section 8 Exceptions

Section 8 of the Data Protection Acts provides for an exception to the normal rules on disclosure in a number of specified instances: for example, where information is required urgently to prevent injury to an individual.

Notifiable Diseases

Certain infectious diseases are subject to specific regulations, designed to protect public health.¹⁹

Other Statutory and Legally Permitted or Required Disclosures

A person holding personal health information may also be authorized or required to release personal health information without legal liability in certain instances. For example, the Health (Provision of Information) Act 1997 provides an exemption from the disclosure rules of the Data Protection Acts for information disclosed to the National Cancer Registry. Another example is the Persons Reporting Child Abuse Act 1998 which provides immunity from civil liability to any person, acting reasonably and in good faith, who reports (in line with the Act) to designated officers of the HSE or any Garda his or her opinion that a child has been or is being abused.

Legal Proceedings

Confidentiality can also be lost where damages are claimed in a law suit.

Medical Council

The Medical Council has also identified instances where patient consent may be over-riden: for example, when necessary to protect the welfare of society.

2.2.10 Consent and Data Protection

The collection, use and disclosure of personal health information has traditionally been subject to a variety of ethical and common law rules that place an emphasis on

¹⁹ Section 29 of the Health Act 1947: regulations are made by the Minister for Health and Children and the Health Protection Surveillance Centre is the responsible body.

consent and confidentiality. This emphasis is found in the Data Protection Acts and EU Directive.²⁰

2.3 CONCERNS ABOUT USES OF PERSONAL HEALTH INFORMATION AND THE HEALTH SECTOR

Various concerns have been voiced about the need to ensure that the appropriate balance is struck between individual and societal interests in health information.

“Information is the most powerful and valuable resource in contemporary society, but it must be managed properly in order to protect those whose information it is, and in order to maximise the potential benefits to be obtained from the collection and utilisation of such information. Technological advances that enable healthcare to be provided more efficiently and more effectively are clearly to be welcomed, but patients should have the ultimate control over what medical information is shared with other doctors as well as with insurance providers and other companies.”²¹

In 2001, the Irish Data Protection Commissioner stated his belief that:

“... I believe that the handling of medical data within the health sector needs a major overhaul, to ensure that patient data can flow as medical treatment requires, while ensuring that medical confidentiality is accorded utmost priority. It is also important that medical practitioners at every level should have clear guidance on what is and what is not legally permissible.”

There is also increasing awareness among healthcare professionals about information management issues and possible legal consequences. Three factors can be identified as most relevant:

- ◆ there is uncertainty about the nature and scope of the legal and ethical rules governing privacy, confidentiality and security of personal health information.
- ◆ at the same time, individuals in society have become more accustomed to, and aware of, their rights as citizens, consumers and patients.
- ◆ the demands that are placed on the health system are greater and more varied than ever before.

2.4 BALANCING RIGHTS AND INTERESTS

One of the key debates, internationally, in data protection and privacy is the need to balance potentially competing rights and needs. The rights relate to individuals and the degree of control they should enjoy over information relating to them. The needs relate to society and the benefits to the public good that greater use and sharing of information may facilitate. In the health sector, this is sometimes presented as a conflict between the rights of the patient to determine who has access to their medical records and the needs of the health service to use patient information for a range of

²⁰ The UK Information Commissioner stated “there is an overlap ... between the fair processing requirements of the Act and the consent requirements of the common law.”

²¹ Madden D., *Empowering Health Information: Medico-Legal Issues* (2002) 8 MLJI 7

management and research purposes that stand to benefit society generally, through better service planning and healthcare innovations. However, it is also important to acknowledge that individual patients are, in practice, the net beneficiaries of better information management and medical research.

PART 3: THE EXISTING REGULATORY FRAMEWORK

It is essential to consider the current regulatory framework to assess how it impacts upon the health system. Accordingly, this Part looks at the various sources of regulation of personal health information in Ireland.

The Audit Document is particularly useful for anyone interested in reading more about the material covered in this Part and it extends to a consideration of relevant privacy law in selected other countries and at European level.

International and National Framework

The existing regulatory framework relevant to personal health information is shaped by:

- international privacy instruments and agreement,**
- international data protection instruments,**
- European Union Data Protection Directive,**
- national law,**
- ethical codes of healthcare professionals,**
- decisions of (and guidance issued) by the Data Protection Commissioner and the Freedom of Information Commissioner and Courts.**

3.1.1 International Privacy Instruments and Agreements

The most important of these instruments, declarations and agreements are enumerated below. They are dealt with individually in the accompanying Literature Review but collectively they have the common theme of respect for the individual and his or her privacy.

- Universal Declaration on Human Rights (1948)*
- European Convention on Human Rights & Fundamental Freedoms (1950)*
- International Covenant on Civil & Political Rights (1966)*
- Charter of Fundamental Rights of the EU (2000) (2000/C 364/01)*
- Universal Declaration on Bioethics and Human Rights (2005)*
- 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)*

-Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Biomedical Research' (No. 195) (2005)

3.2.2 International Data Protection Instruments

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

- Organisation for Economic Co-operation & Development's 1980 Guidelines Governing the Protection of Privacy & Transborder Flows of Personal Data.

-Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data.

There are also two (non-binding) information related Council of Europe Recommendations relevant to the health sector dealing with medical databanks²² and the protection of medical and genetic data²³.

3.2 EU Directive on Data Protection

The EU Directive on Data Protection (95/46/EC) was developed in the context of creating the infrastructure necessary for the completion of the Internal Market. It sets a baseline common level of privacy in EU Member States and was implemented by the Data Protection Act 2003.

3.4 National Law²⁴

Relevant here are-

- the Constitution,
- Legislation, and
- Common Law Duties of Confidentiality.

3.4.1 The Constitution

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.

3.4.2.1 Legislation

The main Acts, with accompanying Regulations, relevant to health information management are:

- Data Protection Acts 1988 & 2003
- Data Protection (Access Modification) (Health) Regulations 1989²⁵
- Freedom of Information Acts 1997 & 2003
- Freedom of Information Act, 1997 (Classes of Health Professionals) Regulations 2001²⁶
- Freedom of Information Act, 1997 (Section 28(6)) Regulations 1999²⁷

²² Council of Europe Recommendation, R(81)1, on *Automated Medical Databanks*.

²³ Council of Europe Recommendation, R(97)5, on the *Protection of Medical Data*.

²⁴ Part 3 of the Audit document also sets out information on the national law in Ireland.

²⁵ SI No. 82 of 1989

²⁶ SI No. 368 of 2001

- Health (Provision of Information) Act 1997
- European Convention on Human Rights Act 2003
- Health Act 2007
- Disability Act 2005
- Statistics Act 1993
- Social Welfare Acts 1998 and 2002

On account of their importance to the regulation of health information, the Data Protection Acts and Freedom of Information Acts are discussed below in some detail. Information on the other statutes referred to above is contained in Part 2 of the Audit document.

Data Protection Acts 1988 & 2003

The Data Protection Act 1988 gave effect to the 1981 Council of Europe Convention while the 2003 Act implemented the 1995 EU Data Protection Directive. The later Act strengthened individuals' (data subjects') rights in relation to their personal information and imposed more obligations on those that keep such information (data controllers).

Personal Data

Personal data means any information (including an opinion or comment) about a living individual who is capable of being identified, either from that information or from that information in conjunction with any other information currently in the possession of or likely to come into the possession of the data controller.²⁸

Accordingly, the definition of personal information applies only to natural persons and does not apply to deceased individuals.

The EU Directive does not expressly confine itself to living persons (see Article 2a) and the matter of including deceased individuals within Irish data protection coverage was considered during the course of preparing the Data Protection Act 2003, but apparently there was not significant public interest in doing so.²⁹ However, in the context of personal health information, the issue of protecting medical records following the death of an individual needs to be considered -this is separate from the issue of the right of access of a family member to a deceased person's records which is dealt with below as one of the differences between FOI and data protection legislation.

This would mean that personal health information of a deceased individual would enjoy the quality principles (relating to collection, use, disclosure etc) as applied to information relating to a living individual.

In the USA, the concept of "survivor privacy" has been upheld by the Supreme Court; this can work to protect records of a deceased person on the basis that their release would be upsetting to the family of the deceased. It may be that this notion of "survivor privacy" is an aspect of the protection of private and family life under article 8 of the European Convention on Human Rights.

²⁷ SI No. 47 of 1999

²⁸ Section 1 of the Data Protection Acts 1988 and 2003

²⁹ Data Protection Bill 1987, Dáil Éireann, Second Stage, Vol.375, 17 November 1987.

Sensitive Personal Data

Irish data protection legislation recognises that certain categories of personal information require higher standards of protection from those who seek to obtain, hold, use or disclose them. These are the so-called categories of sensitive information and include personal health information. While there is no definition of personal health information in the Data Protection Acts, a survey of other jurisdictions³⁰ indicates that it is likely to encompass recorded information (including opinions, assessments and intentions) about a living identifiable individual relating to:

- ◆ any aspect of the physical or mental health of the individual, as well as any genetic data or human tissue data that could be predictive of the health of the individual, or his or her relatives or descendants;
- ◆ the actual, required or intended provision of healthcare to the individual.
- ◆ the individual's express wishes about the future provision of health services to him or her;
- ◆ payment for healthcare provided to the individual and medical insurance details;
- ◆ any identification number, symbol or other reference assigned to the individual, intended to assist the provision of healthcare services to the individual or generally;
- ◆ any other identifying information about the individual that is collected in the course of, or is incidental to, the provision of healthcare, even though (on its own) it may not be obviously health information – this would include such basic information as name, age, sex and other personal information, such as employment and social circumstances.

Given its wide-ranging nature, personal health information is collected, recorded and used in a variety of situations and by numerous types of data controllers. A health agency may collect it from applicants to establish eligibility or suitability for particular services. Hospitals obtain and keep information on admissions, treatments, discharges and so forth. Similarly, healthcare professionals, like GPs, opticians, dentists, etc., also keep relevant client health records. For risk assessment reasons, an insurance company may require that an applicant for a policy undertake a medical examination. For other reasons, a school or college legitimately may record certain health information on its students.

Genetic Data

Advances in medical technologies have given rise to new privacy concerns in relation to the significance and impact of ***genetic tests and the processing of genetic data***.

³⁰ Some countries have specific Health Information Acts. For example, where there is no Federal Health Information Act in either Australia or Canada, several States and Provinces, respectively, have such specific legislation. These are considered in Part 6 of this Paper in the context of formulating a new definition for “personal health information” in the proposed Health Information Bill.

The independent advisory Working Party set up under Article 29 of the EU Data Protection Directive produced a *Working Document on Genetic Data*,³¹ which outlines the privacy issues and implications arising from genetic testing and the processing of genetic data. The Working Party also considered the extent to which genetic data is protected by the EU Data Protection Directive and felt that there was no doubt that genetic data is personal data under the Directive.

Most recently published international instruments forbid any discrimination based on genetic data. Under Article 21 of the Charter of Fundamental Rights of the EU, “any discrimination based (...) on genetic features” shall be prohibited.³²

The matter of genetic testing has received some legislative attention in Ireland (see the Disability Act 2005 in Audit Paper) and also under Regulations³³ made in September 2007 by the Minister for Justice under the Data Protection Acts. The Regulations provide that the processing of genetic data in relation to the employment of a person can only take place with the prior approval of the Data Protection Commissioner.

Rights

Under the *Data Protection Acts*, an individual has the right to:

- ◆ Have information processed fairly (the fair processing principle)
- ◆ Prohibit the use of his or her information for direct marketing,
- ◆ Establish whether any person is a data controller,
- ◆ Establish whether a data controller (or the data controller’s agent) keeps personal data on him or her, and if so, be supplied with the personal information concerned in an intelligible format together with details on:
 - ◇ the purposes for which the information is kept.
 - ◇ the persons to whom such information has been, or may be, disclosed.
 - ◇ the types of information concerned and any information on the sources of such information.
 - ◇ the logic involved where the processing of the personal information by automated means has formed or is likely to constitute the sole basis for any significant decision relating to the data subject. (This could be relevant to the health sector, for example, where a decision to treat was based solely on an automated risk scoring system for a chronic disease.)

³¹ Article 29 Working Party (17 March 2004)

³² This prohibition can also be found in the Council of Europe’s Convention on Human Rights & Bio-Medicine (Article 11) and UNESCO’s Universal Declaration on Human Genome & Human Rights (Article 6).

³³ S.I. No. 687 of 2007 - Data Protection (Processing of Genetic Data) Regulations 2007

◆ Have his or her personal information enhanced, corrected, blocked (that is, having personal information marked so as to ensure that it cannot be used for certain particular purposes)³⁴ or otherwise amended (including by deletion where this is not inconsistent with the keeping of a proper record), if it is held in contravention of the data protection principles and, where any of these actions materially modifies the information kept, there is a further requirement on the data controller to notify any person to whom the data were disclosed in the previous 12 months unless such notification proves impossible or involves disproportionate effort.

◆ Object to the processing of personal data relating to him or her in certain circumstances particularly where such processing is likely to cause distress.

Subject Access to His or Her Health Information

The 1989 Data Protection (Access Modification) (Health) Regulations set out the access rules in relation to an individual's entitlement to access his or her health information. They provide that such information shall not be supplied by, or on behalf of, the person holding it to the individual concerned, if it would be likely to cause serious harm to the physical or mental health of the individual. However, nothing in that prohibition excuses the person holding the information from supplying so much of the information sought as can be supplied without causing the harm referred to in that stipulation. If the person keeping the information is a health professional, then he or she can make the access decision. Where the person is not a "health professional", the Regulations require that he or she may not communicate the information requested until after consulting with an "appropriate health professional".

Freedom of Information Acts 1997 & 2003

Unlike in most other countries with Freedom of Information and Privacy/Data Protection laws, Irish legislation give individuals separate rights of access to their personal information³⁵.

Rights

The FOI Acts 1997 & 2003 apply to public bodies and give individuals legal rights to:

- 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

Personal Information

Personal information is defined in the Freedom of Information Acts as "information (including views and opinions) about an identifiable individual that -

³⁴ The example of potential blocking given on the Data Protection Commissioner's website is "you might want your data blocked for research purposes where it held for other purposes".

³⁵ In the Oireachtas debates on the then Freedom of Information Bill 1996, it was stressed "that personal privacy is strongly protected by this Bill. People will not be able to see private information about other people" Minister of State at the Department of Enterprise and Employment, Seanad Eireann, 29 January 1997.

(a) would, in the ordinary course of events, be known only to the individual or members of the family, or friends, of the individual , **or**

(b) is held by a public body on the understanding that it would be treated by it as confidential"

One of the illustrative examples used in the Act is “information relating to the educational, medical, psychiatric or psychological history of the individual”.

Subject Access Rights to His or Her Information

As regards an individual accessing his or her health information, section 28(3) which relates access to medical, psychiatric and social work records, makes provision for denying access where, in the opinion of the public body, to release the record might be prejudicial to the subject’s physical or mental health, well-being or emotional condition.

This differs from the corresponding provisions in data protection law. The obligation on the public body to refuse access is discretionary under the Freedom of Information Acts, whereas it is mandatory on the data controller under the Data Protection Access Regulations. There is also a difference in the degree of potential harm to the requester justifying denial of access, with freedom of information law requiring a lower threshold. Further, under section 28(4), the public body to which the access request is made is required to advise the requestor that where access is denied under section 28(3) it may be provided through a nominated health professional.

The 2001 FOI Regulations prescribe classes of health worker and social worker for the purposes of section 28(7) of the Freedom of Information Act (FOI), 1997. Their effect is to widen the meaning of "health professional" in section 28 of the FOI Act to include persons holding certain qualifications in social work or clinical psychology.

The 1999 FOI Regulations prescribe the classes of individual whose records will be made available to parents and guardians, and the classes of requester to whom the records of deceased persons will be made available, having regard to relevant circumstances

and to guidelines published by the Minister for Finance. Concerns with these Regulations are discussed further below.

Differences between Data Protection Acts and FOI Acts

By way of summary, the main similarities and differences applicable to personal information and rights between the Data Protection Acts and the Freedom of Information Acts are set out below.

DIFFERENCES BETWEEN FOI ACTS AND DATA PROTECTION ACTS

FOI does not apply to the private sector except where individuals are providing services as agents of the public sector (for example, GMS GP and medical card patients). Data protection applies to both the private and public sectors.

The FOI Acts do not establish an explicit set of information quality principles applicable to those who 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 protections 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 specific provision in the Data Protection Act 2003 that “a right conferred by this Act shall not prejudice the exercise of a right conferred by the Freedom of Information Act 1997”.³⁶

The length of time for complying with an access request varies -20days 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.

Treatment of Information on Deceased Individuals under both Acts

Access to Information:- A key distinction between the Data Protection and Freedom of Information Codes relates to the treatment of information (especially access) of deceased individuals. As stated above, the definition of personal information in the Data Protection Acts does not apply to deceased individuals.

Despite the absence of express statutory protection under the Data Protection Acts, this is not to say that lower standards should apply to information held on identifiable deceased persons. In that regard, the Medical Council has stated that:

“... the medical records of a deceased person remain confidential and death does not absolve a doctor from the obligation of confidentiality”.³⁷

³⁶ Section 1(5)(a)

Section 28(6) of the FOI Acts provides that the Minister for Finance may make regulations providing for access where, inter alia, the individual to whom the record relates is dead and the requester is a member of a class specified in the Regulations. Such Regulations were made in 1999³⁸ and prescribe (i) the classes of individual whose records will be made available and (ii) the persons to whom those records will be made available, having regard to relevant circumstances and to guidelines published by the Minister.

The Information Commissioner has commented in her recent Annual Reports on drafting problems with these Regulations. The net effect is that, in her view, the wording of the 1999 Regulations as they stand provides for access to records of deceased persons by any requester who is defined in the Regulations as a next of kin of the deceased person. A next of kin as provided for in the 1999 Regulations includes partners and former partners, and has no regard to the status or currency of the relationship between the next of kin requester and the deceased person to whose records access has been sought. She has stated her opinion that the 1999 Regulations need to be re-drafted.

As one of the principal goals of the Health Information Bill is to achieve clarity and consistency, it is important these objectives are realized in the sensitive area of respecting the privacy of a deceased individual while acknowledging the legitimate interest of a spouse or another close family member. In most cases, the interests of the family will not extend further than the need for such information as is necessary to assure them that proper care was provided. However, in some instances, the nature of the illness that led to the death of the individual concerned might have health or genetic implications for other family members (that may extend well beyond immediate blood relatives). A common sense approach, based primarily on prior explicit consent, may be desirable in the majority of cases but the range of potential scenarios offers a legislative challenge that has to be met.

Parents and Children

The Data Protection Acts do not address expressly, in any way, the position of parents or guardians in relation to personal information held on their children. Section 28(6) of the FOI Acts –and the 1999 Regulations- referred to above deal not only with deceased individuals but also with parents and guardians. There has also been judicial consideration of the matter in the Mc K case (see 3.7 below).

However, even under FOI, there is a lack of clarity on subject access to health records of minors: including, at what age does a minor have the right to privacy vis à vis a parent in relation to his or her health information? what are the rights of a separated parent or guardian to access such information, particularly where the other parent or guardian opposes access? and should social work (including child protection) records be treated in the same way as are health/medical records?

³⁷ Medical Council Guidelines on Ethical Conduct and Behaviour (2004)

³⁸ The Freedom of Information Act, 1997 (Section 28(6)) Regulations 1999. It is understood that these regulations are currently under review.

3.5 Common Law Duty of Confidence

Confidentiality underpins the healthcare professional-patient relationship but 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 (see below) and by the common law doctrine of confidentiality.

The common law equitable doctrine 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 arising from the healthcare 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.

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. In particular, healthcare professionals may have other ethical duties or legal responsibilities to disclose confidential information, without consent. These exceptions to consent are discussed at the end of the next Part of this Discussion Paper.

3.6 Ethical Codes

The purpose of a professional code of ethics is to set out and promote a body of principles to guide its members' conduct in their relationships with patients, colleagues and society. The Ethical Codes of several healthcare professions are identified in Part 2 of the accompanying Audit document. It will be important that all relevant Ethical Codes be updated in line with any forthcoming health information legislation.

3.7 Decisions of, Guidance given and Comments made by the Information Commissioner and Data Protection Commissioners as well as Judicial Decisions

Both Commissioners have, on numerous occasions, issued guidance and advice on the application of the principles in their respective areas to the health sector. These are available on their websites as are their annual reports which feature health sector

cases. Issues raised by both Commissioners are included in the following Part of this document which deals with matters requiring consideration in preparing the Health Information Bill.

The Courts have been more actively involved in FOI cases than data protection cases. In the health area, the Supreme Court decision in the matter of McK v. the Information Commissioner has important implications for the rights of persons to access the medical records of their children.³⁹ At issue was whether a father, a widower who had been separated from his late wife, who was joint guardian of his children, was entitled under FOI legislation to information, in the form of hospital notes, about an illness of his daughter. The hospital involved had refused access and that decision had been upheld by the Commissioner. In the Supreme Court the decision was overturned and Denham J stated the case “raises fundamental issues on the approach to be taken to an application by a father to access information in medical records of his daughter, a minor, where other guardians object to his accessing such records”. She also observed that “the relationship between parent and child has a special status in Ireland”.

³⁹ Decision of the Supreme Court [289/2004] in the matter of the Freedom of Information Act, 1997 between N. McK, Appellant, and the Information Commissioner, Respondent. (24 January 2006)

APPENDIX 1: ELECTRONIC HEALTH RECORDS

It is argued that the development of EHRs will significantly enhance the effectiveness and efficiency of health care for the individual patient⁴⁰ and the system generally, for example in providing better research data⁴¹. One definition is set out below.

The Integrated Care EHR (ICEHR) is defined as a repository of information regarding the health status of a subject of care in computer processable form, stored and transmitted securely, and accessible by multiple authorised users. It has a standardised or commonly agreed logical information model which is independent of EHR systems. Its primary purpose is the support of continuing, efficient and quality integrated health care and it contains information which is retrospective, concurrent, and prospective.

Definition by the International Standards Organisation in Health informatics — Electronic Health Record — Definition, scope, and context⁴²

Specifically, the benefits claimed⁴³ for EHRs are that they are an appropriate means to:

- bring about better quality of treatment because of better information about the patient;
- reduce medical errors and adverse health events,
- create a better understanding of health information through developing stronger partnerships between consumers and health care providers,
- medical histories will not have to be repeated with every visit to a medical practitioner saving time and reducing the possibility that the patient will fail to recall relevant facts or symptoms,
- augment the security of patient information,
- improve the cost efficiency of medical treatments and thus prevent further rapid growth of health care budget deficits;

⁴⁰ The Commission on the Future of Health Care in Canada advocated EHRs for all Canadians and noted that “[d]iagnoses, treatments and results can be improved when health care providers have access to complete personal health information and can link that information to clinical support tools.”

⁴¹ See, for example, 13 D. J. Willison, et al. “Patient consent preferences for research uses of information in electronic medical records: interview and survey data” (2003) 326 *British Medical Journal* 373.

⁴² ISO TC 215 (2005)

⁴³ *Electronic Health Records and the Personal Information Protection and Electronic Documents Act: Report prepared by University of Alberta, Health Law Institute and University of Victoria, School of Health Information Science (April 2005)*

- furnish the necessary data for quality control, statistics and planning in the public health care sector which should also have a positive effect on public health care budgets,
- in the case of EHRs available to patients, can provide them with convenient access to their own health information and facilitate activities such as prescription renewals and appointment booking.

It would be misleading to give the impression that there is universal agreement on the merits of EHR systems. Some commentators question the claim that EHRs will improve completeness and accuracy of data. Further, a Canadian study found that “there is little to no empirical research and analysis of how EHRs will improve healthcare, and what research exists suggest that comprehensive EHRs may not be the best solution.” In addition, in an era of identity thefts, while EHRs offer the potential for greater security, audit trails and authentication measures, they also increase the level of unquestioning reliance on their accuracy. There is also the question of cost: the EHR system being developed by the NHS for England has a current cost estimate in excess of £12Bn

Privacy Concerns and Legal Basis for EHR System

By their very nature, EHRs raise concerns regarding the privacy, confidentiality and security of health information. This has led directly to a consideration of the legal basis for establishing such systems in a privacy context by the EU Working Party established under Article 29 of the EU Data Protection Directive. The Working Party issued a draft paper (for public comment in January 2007)⁴⁴ which provided guidance on the interpretation of the applicable data protection legal framework for EHR systems.

On the privacy angle, the Working Party:

- made it clear that “EHR systems introduce a new risk scenario, changing the whole scale of possible misuse of medical information about individuals”,
- added that some also fear the “function creep” phenomenon, in which uses of EHRs will expand over time to encompass activities not originally foreseen, including matching EHRs with other personal information databases,
- and observed that “the creation of comprehensive records may generate increased interest in others to obtain access to those records”.

The Working Party also set out the data protection framework, applicable under the EU Directive, for processing information in an EHR (where processing covers all aspects of information management from collection, use, retention, disclosure, transfer and security as well as the individual’s right to access and correct his or her information and object to and block its use). The document states that all such information in an EHR is sensitive within the meaning of the Directive and cannot be processed unless one or more of the following conditions is met: namely-

⁴⁴ Working Document on..... The Article 29 Working Party is composed of representatives of the national data protection authorities (DPA), the EDPS and the European Commission.

- explicit consent (which must be free, specific and informed) (Article 8.1)
- vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his or her consent and the processing must relate to essential individual interests (Article 8.2),
- processing of medical data by health professionals which only covers processing of personal data required (and not just useful) for the specific purpose of (Article 8.3)⁴⁵,
- subject to the provision of suitable safeguards, substantial public interests (Article 8.4)

The Working Party document then examined the issues (mainly legal) that are associated with each of the above in terms of creating a suitable EHR framework and concluded that given practical issues associated with consent Article 8(4) of the Directive “could, therefore, serve as a legal basis for EHR systems, provided that all the conditions mentioned [in the Article and Recital 34] are fulfilled”. In particular, suitable safeguards for the protection of personal data in an EHR system must be provided for: in particular, respect for self-determination by individuals (opting in and/or opting out).

The Article 29 Working Party concluded that “considering the impact of EHR systems and the special need for transparency of such systems the safeguards should preferably be laid down in a special comprehensive legal framework.”

Other Countries

In terms of EHR systems, only the NHS for England has moved from conception and design to implementation and even there the system is still at an early stage of implementation. It is also worth making the point that, despite early promises, there is an emerging realisation⁴⁶ that a single integrated record may not be practical. For that reason, other countries are seeking to link multiple pockets of electronic health information into some alternative workable formation to help provide better care.

Australia

The Australia national strategy for developing the country’s e-health agenda is called *HealthConnect*.⁴⁷ The expectation is that by end 2008, Australia will be well advanced in achieving the goal of electronic connectivity between all major health institutions and health care providers.⁴⁸ Underpinning every aspect of the e-health strategy is consent, voluntary participation and opt-in arrangements for individuals. For example, even where patients opt-in, they will be able still to request that an event summary is not entered onto the system with respect to a particular health consultation.

⁴⁵ The WP state that this does not include research which is not even mentioned in Article 8.3. It is worth noting that “medical research” appears to have slipped into the applicable provision (section 2B(4)) in the Data Protection Acts 1988-2003.

⁴⁶ See, New Zealand Health Information Strategy (2005) where it stated that “EHRs are recognised as a virtual concept that relies on a network approach, where data is pulled together from multiple data stores. It is no longer viewed as a single physical repository”.

⁴⁷ For a full description of HealthConnect and related issues, see www.healthconnect.gov.au

⁴⁸ <http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/whats-happening-1lp>

It is proposed that the HealthConnect EHR “will not replace providers’ own clinical records or clinical information systems. Providers will continue to maintain their own consumer health records but may choose to incorporate selected HealthConnect EHR information in their records or clinical information systems.”⁴⁹

The Australian national e-health programme known as HealthConnect is based on consent, voluntary participation and opt-in arrangements.

The National E-Health Transition Authority (NEHTA)⁵⁰ was established in 2005 to develop better ways of electronically collecting and securely exchanging health information. It is currently establishing the national foundations to the planned Shared Electronic Health Records system (SEHRs). The Authority has stated that:

- the primary purpose of the EHR will be to improve the quality and safety of healthcare experiences,
- the secondary purposes of the EHR include public health and policy planning, and supporting safety initiatives, disease detection, research and education.⁵¹

The Australian national EHR approach will involve the creation of one (or more) EHR Service(s), which will maintain, and provide access to, the EHR of those individuals who choose to participate in that Service. Healthcare providers and organisations will be able to contribute information to an individual’s EHR by keeping electronic records of patient interactions, and using software which is compatible with the EHR Service(s). This software will allow healthcare providers to maintain their own detailed records, while ensuring that the most critical information can be easily included in the individual’s EHR, without the need for double data entry. Providers will also be able to see summarised views from the individual’s EHR.

Health Connect believes the voluntary nature of the scheme is necessary for patient acceptance even though it recognises that the freedom to participate raises issues with respect to the usefulness of the records not only for an individual’s primary care but also for secondary uses.

Canada

Canada Health Infoway is the government corporation charged with promoting “the development and adoption of electronic health information systems with compatible standards and communications technologies on a pan-Canadian basis with tangible benefits to Canadians”.⁵² At present, EHR systems are at various stages of development at federal and Province level across Canada.⁵³

⁴⁹ HealthConnect 2004a, 2

⁵⁰ www.nehta.gov.au

⁵¹ Several Australian government and Australian government-commissioned reports have emphasized the potential contribution of shared EHRs to population health monitoring and research. For example, as early as 2000, the National Electronic Health Records Taskforce pointed to evidence of the consumer benefits of shared EHRs for population and medical research.

⁵² See Canada Health Infoway mission statement online:

www.canadahealthinfoway.ca/aboutinfoway/vision.php?lang=en

⁵³ For a comprehensive summary of such initiatives in jurisdictions across Canada, see Health Canada, Towards an Evaluation Framework for Electronic Health Records: An Inventory of Electronic Health

“Canada Health Infoway should ... be responsible for developing a pan-Canadian electronic health record framework built upon provincial systems, including ensuring the interoperability of current electronic health information systems and addressing issues such as security standards and harmonizing privacy policies.”

The Romanow Commission Report⁵⁴

The eventual goal is to establish an EHR system that provides seamless access to personal health information wherever a patient may be in the country. This vision necessarily involves the transfer of patient information across provincial/territorial borders, a fact that is important in considering the application of different National and Province laws on privacy.

Some commentators, in Canada, have criticized the slow pace of EHR development. In 2005, the Health Council of Canada recommended “rapid adoption” of EHRs and telehealth technologies “as tools to improve access, quality and comprehensiveness of health care”⁵⁵ and lamented the fact that “[o]n the current path and timetable only half the country will have electronic health records by 2009 but the remainder may wait until 2020”⁵⁶

No final decision has yet been made on whether Canada (either nationally or at Province level) will have an opt-in or opt-out model. However, the Alberta Government was forced to repeal legislation requiring an opt-in approach to electronic health record because it was claimed to be unworkable.

New Zealand

New Zealand has a high level of computerization in its healthcare system upon which to develop an EHR system. For example, almost 100% of general practices employ practice management software, with most using it for maintaining cervical screening, diabetes, breast screening, asthma, and blood pressure registries and over 90% of general practices utilize electronic messaging.⁵⁷

The ***Health Information Strategy for New Zealand*** (2005) constitutes the most recent national strategic statement regarding electronic health records.⁵⁸ The strategy rejected “a single integrated record [. . . as] neither workable nor practicable”. Instead, it has adopted what it describes as a distributed electronic health record that consists of: local systems for direct clinical care, which are owned and operated by

Records Initiatives Across Canada (March 2004), prepared by Doreen Neville et al., online: <http://www.hc-sc.gc.ca>

⁵⁴ The Romanow Commission Report *Building on Values: The Future of Healthcare in Canada* (2002)

⁵⁵ Health Council of Canada, *Health Care Renewal in Canada: Accelerating Change* (January 2005) at 41, online:

http://hcc-ccs.com/report/Annual_Report/Accelerating_Change_HCC_2005.pdf

⁵⁶ 34 Michael Decker, *The Electronic Health Record: What it is and why you should want one!* (14 February 2005), online: Health Council of Canada <<http://hcc-ccs.com/article1.aspx>>.

⁵⁷ Didham R, Dovey S, Barker L *Information technology systems in general practice* (2005) Wellington: New Zealand

Health Information Service

⁵⁸ NZ Ministry of Health (August)2005

healthcare service providers and may vary among providers; regional systems for coordination of care and decision-making about service delivery; and national systems, which include individual health event-and health topic-specific data collections. Data held in local, regional, and national systems rely on the National Health Index number, which enables linkage at the individual patient level when allowable. (The National Health Index Number is discussed later in this Part in the Unique Health Identifier section.)

England and Wales

The NHS for England and Wales has the most developed EHR system in the world. It is designed to be “...a cradle-to-grave NHS Care Record for each patient, which will transcend traditional care organisations’ boundaries”.⁵⁹ However, its development has been controversial on a number of fronts, in particular costs, consultation process, lack of direction, delays, privacy and security.⁶⁰

The EHR system is part of the National Programme for Information and Technology (NpFIT). A new body -***NHS Connecting for Health***- was established, as an agency of the Department of Health, in April 2005 with the stated primary role of delivering the NpFIT.⁶¹

Connecting for Health has a number of related elements⁶²: including, linking more than 30,000 GPs to nearly 300 hospitals by 2014, an online booking system, e-prescriptions, fast computer network links between NHS organisations and a centralised electronic medical records system for 50m patients. In June 2007, the National Audit Office estimated that the total IT bill was set to be £12.4bn.⁶³

The electronic health record will include:

- personal health information—e.g. drug allergies; details of operations and/or conditions; medication history; pathology, radiology and other results and a summary of contacts with care providers,
- demographic data—e.g. address details, held nationally and accessible through local systems,
- a unique identifying NHS number, which will also form the common link between personal health information and demographic data.

The system will have two patient records: the Summary Care Record and the detailed record. The former is a summary of an individual’s key health information that will be

⁵⁹ NHS National Programme for Information Technology 2004.

⁶⁰ For example, in April 2007, the British Public Accounts Committee reported on the National Programme that "urgent remedial action is needed at the highest level if the long-term interests of NHS patients and taxpayers are to be protected."

⁶¹ See www.connectingforhealth.nhs.uk

⁶² Technically, the System has been designed around a national repository of health information with principal system elements providing secure data access and messaging throughout England (known as the Spine), plus other system elements which provide key services.

⁶³ This includes the original £6.2bn cost of contract, which has now risen to £6.8bn due to the scope of the programme extending, and various other costs incurred from training people and paying for NHS trusts to implement the new systems.

available to treating healthcare professionals. It will contain details on medications, allergies and adverse reactions to medicines and any additional information held with the consent of the individual concerned.

Individuals have three choices for limiting access to their Summary Care Record as follows: they can request that-

- certain information not be included,
- the Summary Care Record be created but not accessible by anyone outside the GP surgery without explicit consent, or
- no Summary Care Record be created.

When the system is more fully developed, it is planned that there will be another option. Individuals will be able to choose to prevent specific information from being visible without express consent by utilising what will be called a 'sealed envelope'. This might be used by an individual to prevent access to health information he or she considers very sensitive, for example, psychiatric or sexual health information.

The system is opt-out to the extent that the individual is advised that the record is being created and will be shared unless he or she responds otherwise. Where there is a Summary Record, NHS staff will have to have a legitimate relationship with the patient to access his or her data. Given the usual unplanned and un-referred attendance at A & E Departments, clinicians in A&E are some of the few NHS staff able to create an immediate legitimate relationship with the patient and thereby gain access to the Summary Care Record. All access to the Summary Care Record will be logged and unusual access will be investigated by a member of staff in every NHS Trust - often known as the Caldicott or Information Guardian. Individuals can request a copy of the audit log relating to their Summary Records.

Detailed Records are linked medical records generated by healthcare professionals locally throughout the system and the patient will be able to choose what information is available to those treating him or her.

The NHS's development and deployment of electronic health records and electronic patient records has been accompanied by recognition of their potential for population-based monitoring and research. EHRs were also recognized as essential in the further development of population-based disease registries.⁶⁴

⁶⁴ "Implementing Information For Health: Even More Challenging Than Expected?" by Denis Protti (June 2002)

APPENDIX 2: UNIQUE HEALTHCARE IDENTIFIERS

In order to effectively connect patient records held separately by GPs, hospitals etc, e-health systems must be able to successfully and uniquely identify individuals to ensure the right information is assigned to the right individual. The adoption and use of a unique healthcare identifier (UHI) for patients and a similar concept identifier for healthcare providers is arguably essential to ensure the accurate identification of individuals occurs across all healthcare settings. It should be noted that while UHIs are certainly an essential building block in any EHR system they also have their own separate uses and distinct considerations.

UHIs for patients generally have the following features:

- a summary record: identifier, name, date of birth;
- an identification record: summary record information, plus further identifying information such as address; and
- a demographic record: identification record information, plus additional data fields such as mobile phone number.

The above three tiered structure provides functional limitation, and segregates parts of the record holding different, and more detailed, personal information. As the purpose of an identifier is to identify there is no need for clinical information to be held and such information is normally not held on or by the identifier system.

The Benefits of a Unique Health Identifier for Patients

The National Health Information Strategy outlined the case for a UHI. It argued that “unique identification promotes the quality and safety of client/patient care in many ways”: including-

- providing for a more definite association to be made between the client/patient and his/her records which in turn promotes client/patient safety through the correct identification of the individual;
 - as a key requirement for the proper implementation of the electronic healthcare record upon which many other benefits will accrue⁶⁵;
 - supporting the provision of shared care; and
 - enabling good record management that in turn supports clinical audit and risk management processes
-
- largely obviating the need for clients/patients to provide personal details at every contact with the health service, a procedure that clients/patients can find quite irksome, unnecessary and time consuming;
 - allowing the identification of duplicates from repeat contacts by the same individual with primary and secondary care services. This is an essential requirement for epidemiological purposes, screening and

⁶⁵ see *Quality and Fairness: A Health System for You (2001)* – Action 118

vaccination services, in service planning and evaluation and in the management of waiting lists etc;

- supporting the tracking and recall of patients or products if necessary, e.g. for vaccines, medical devices and blood products; and
- reducing wastage of resources, e.g. by reducing the number of repeated diagnostic tests.

Options for unique health identification in Ireland

Since a national approach to unique identification is therefore essential and the two main approaches are the:

- utilisation of the Personal Public Services Number⁶⁶ (PPS Number) together with its supporting inter-sectoral infrastructure;
- development of an entirely separate national identifier that is specific to the health sector and uses its own supporting infrastructure, or
- adoption of new multi-purpose identifier.

The Health Information Strategy considered the first two options above and opted for an identifier “which is based upon the PPS Number and its supportive infrastructure”⁶⁷. A key consideration in this area was the need to recognise the marked interplay between the public and private health sectors.

Towards 2016 and Department of Finance Identity Management Proposals

The current national social and economic partnership agreement *Towards 2016* expressed the view that:

“The development of a system of unique identification for the health service will be considered in the context of a public service wide approach to the development and use of unique identifiers, proposals for which will include discussion with the health sector.”⁶⁸

The Department of Finance is currently considering the development of a public service wide system for identity management purposes. It is concerned primarily with how public sector agencies identify people, how agencies can establish basic facts about people with whom they are dealing, and how people can prove their identity when accessing services remotely.

This will see further consideration of the possible use of the PPSN or any other single identification number (SIN) across all of the public service. The case for and against an alternative sectoral based approach would also be considered.

⁶⁶ The PPS Number is managed by the Department of Social and Family Affairs and use of the PPS Number within the Reach/eBroker framework is in line with the general policy of Government in encouraging its use. The PPS Number is already in use by the GMS (Payments) Board for Medical Cards and the Drugs Payments Scheme

⁶⁷ Action 16, Chapter 12

⁶⁸ *Towards 2016: Ten-Year Framework Social Partnership Agreement 2006-2015* (page 59)

It is reasonable that developing a scheme of unique identification for the health services should build on and be consistent with any proposals that might emerge from the Department of Finance initiative. Equally, it will also be important to consider differentiating, as they have in New Zealand and Australia, between unique identification for access to health services, on the one hand, and for clinical records, on the other.

Privacy Concerns

Controversy over the adoption of a unique health identifier for individuals has focused, to a large degree, on privacy concerns. Arguments about such identifiers are invariably tied up with the greater debate on the allocation, use and abuse of wider-ranging universal State backed Unique Personal Identifiers (UPIs) which raise wider privacy and human rights concerns. In his Annual Report for 1999-2000⁶⁹, the Privacy Commissioner of Canada summed up his fears about the introduction and use of compulsory State backed universal personal identifiers:

“A universal system of identification threatens to undermine our control by allowing organizations to use the identifier to obtain information about us without our knowledge or consent. It greatly increases governments' ability to gather information from various sources and assemble profiles, as well as to monitor and track an individual's behaviour.”

However, the Canadian Privacy Commissioner's Office has also recognized the benefits of unique identifiers in the health system:

“...where a unique health identifier (UHI) for individuals may have much potential to ensure that individuals receive the correct treatment or medicine. The costs in terms of death and injury to individuals due to poor information flows in the health system are relatively well acknowledged. A UHI may address such issues by providing a mechanism that accurately and reliably ensures that individuals are linked to important health information about them.

The challenge was:

“...to ensure that such a highly reliable identifier is not usurped for purposes beyond the health system and the clinical care of individuals.”

In similar fashion to his Canadian counterpart, the Data Protection Commissioner has also expressed concerns about the use of the PPSN as a Unique Health Identifier: primarily, “the very real possibility that it could become a National Identification number by stealth...”⁷⁰ The Commissioner made it clear that he had no difficulty with the introduction by the government of a unique health identity number – combined with sufficient safeguards- on the basis of properly debated and enacted stand-alone legislation.

Identifying Approved Uses of an Identifier for Individuals

It is clear that any adoption of a UHI would make it necessary to expressly prohibit uses of the individual identifier outside the health care system. This leaves open the

⁶⁹ See website: www.privcom.gc.ca

⁷⁰ Appendix 3, The PPSN as a Unique Personal Health Identifier Number

question of what uses within the health care system might be approved or prohibited as well as the need to define the boundaries of the health care system.

It is also generally agreed that, at the very least, any identifier must not:

- contain substantive information about an individual;
- be used to establish a single national data base of all health records;
- be used as a basis for a national identity card system; and

that the individual should have the right to object to having a UHI generally or to block its use for particular purposes or disclosures.

Criteria for Evaluation of Possible Identifiers

Irrespective of the merits of adopting or rejecting a unique health identifier, there is consensus that the criteria underlying the selection of any identifier should include not just privacy considerations but also ones of practicality and cost effectiveness.⁷¹

Other Countries

As is evident from the above, the debate on UHIs can be an emotive one and usually strongly influenced by a country's particular legal history and cultural traditions.

Australia

Currently, in Australia, there is no national system for unique identification of its citizens or residents. There is, however, a Medicare number system which exists to enable reimbursement for healthcare provider fees.

A 2004 population-based survey found that 57% of respondents agreed that “to enable the government to better track the use of health services, all individuals should be allocated a number and that numbers should be used when accessing any health service or facility”,⁷²

In Australia, as in other countries, the development of the UHI is linked closely to work on the Electronic Records System. NEHTA is developing the requirements for a unique, nationally applicable Individual Healthcare Identifier (IHI) and the privacy issues associated with it have been detailed in a Blueprint Document circulated for comment in December 2006.⁷³ The IHI will form part of the Unique Healthcare Identifier Services (UHI Services) which is made up of two separate identification services: namely:

- the Healthcare Provider Identifier (HPI) Service which will uniquely identify healthcare providers, the organisation(s) they work for, and their workplace locations; and

⁷¹ *Unique Patient Identifiers: What are the Options?* Journal of AHIMA, October 1999. Available at <http://www.ahima.org/journal/features/feature.9910.2.html>

⁷² *Community Attitudes Towards Privacy 2004* (June 2004) Prepared by Roy Morgan Research for the Office of the Federal Privacy Commissioner.

⁷³ Privacy Blueprint - Unique Healthcare Identifiers v1.0 1645 18/12/2006 NEHTA

- the Individual Healthcare Identifier (IHI) will be used to uniquely identify an individual in a healthcare setting and to link them correctly to their health information.

The IHI will consist of two parts — a number and a record of information. The record of information will be divided into three sections - a summary record, an identification record, and a demographic record. The summary record will contain the mini-mum number of data fields to enable the matching of an individual to their IHI e.g. name and date of birth. The identification record contains all of the data fields in the summary record and includes additional data fields required for the positive identification and association of an individual with their IHI. The demographic record contains all the data fields used for the summary and identification records, and includes data fields not essential to accurately identify an individual, but which could assist in the provision of quality healthcare (e.g. an individual's mobile phone number could be part of his or her demographic record).

It is intended that everyone using health services will be given an IHI. (This will be separate from and in addition to the Medicare number system.) However, all health services will still be available for use without it. There will be no clinical information on the IHI record and it will comply with the Commonwealth Privacy Act 1988.

New Zealand

The Privacy Act 1993 placed restrictions on the use of unique identifiers, and the National Health Index (NHI)⁷⁴ – an online population-based register that includes a unique random generated identifier. The Act safeguards NHI numbers from being used for any purpose other than in conjunction with the provision of health care services, and of information relating to those services. NHI numbers cannot be related to databases from other sectors of economy, or databases used for different purposes. In 2004, the NZ Ministry of Health launched an NHI Upgrade Programme including a series of initiatives to improve information sharing among health and disability services and to promote wider use of the number.

New Zealand is also currently finalising a Health Practitioner Index (HPI) which will be a central source of core information about every registered health practitioner and provider in New Zealand. The overall goal of the HPI is help New Zealand's health sector find better and more secure ways to access and transfer health-related information to improve the health and wellbeing of New Zealanders. The HPI will improve the privacy and security of patient and practitioner information through the ability to better control access to it. The HPI is intended to make it easier for the right information to be made available to the right person. For example, a medical practitioner involved in the care of a particular patient might be able to access certain information about that patient's care, whereas another type of practitioner may not have the authority to view the same information. Having a single consistent system of identifying practitioners makes this possible and helps protect patient privacy in an environment where patient information is increasingly shared between different healthcare providers.

⁷⁴ The register maintains records of names, aliases, addresses and date of birth.

The National Health Index number is an alphanumeric seven digit code intended to serve as a unique identifier “assigned to each person using health and disability support services”.⁷⁵ The NZ Health Information Service estimates that “about 95% of New Zealanders have their own unique NHI number”. It contains demographic details relating to the individual such as name, maiden name, date of birth, sex, residency status, ethnicity, and any medical warnings.

The Index number can be used only by authorized users, such as health services providers, screening programs, and public health programs. Authorized users can only employ the National Health Index number for stipulated purposes: for example, including obtaining information from clinical information systems and accessing the Medical Warnings System. Additionally, the Ministry of Health uses an encrypted National Health Index number for unique identification of individuals on central data bases for statistical purposes.

The NHI database does not contain any clinical information but it is linked to a separate medical warning system that sends electronic alerts to clinicians about possible dangers in a treatment regimen, such as potentially adverse drug interactions.

United Kingdom

The UK (and all its constituent jurisdictions) has had a health service recipient unique identifier since 1948 when the National Health Service (NHS) began. Despite this, its value as a national unique health service recipient identifier was considered severely limited. It had 22 different formats, was liable to transcription error and was not designed for computer use and validation. In 1995, the full implementation of a new NHS recipient unique identifier began under the *New NHS Number Programme*. A phased approach to implementation was adopted: initially, the programme focused on primary care, then secondary care, then purchasing, and then community care.

As part of this process, in England and Wales, from 30 October 2002, newborn babies were given a NHS lifetime healthcare identification number under the so-called NHS Numbers for Babies Scheme. The unique nine-digit reference number⁷⁶ will stay with each child for the rest of his or her life - the key to his or her clinical history and intended to be a complete record of every visit the individual makes to the doctor, every vaccination received and every illness treated. Previously, infants had to wait several weeks for their registration number to come through from the Registrar of Births and Deaths⁷⁷. During that time the child may have undergone tests and treatment in different locations, had their name changed or changed address etc. The new system gives the baby a unique ID number, helping to ensure that personal records are consistent and universally available to NHS staff from day one.

In 2004 the NHS Information Standards Board announced that NHS Trusts would be required to use the NHS number as their unique identifier.⁷⁸

⁷⁵ www.moh.gov.nz

⁷⁶ There are actually 10 digits. The first nine digits are the identifier and the tenth is a validation digit designed to prevent errors when entering the number in electronic databases.

⁷⁷ Under the new system, NHS numbers will be issued centrally and allocated to babies as close to birth as possible as part of the Birth Notification process carried out by midwives.

⁷⁸ Department of Health 2001 Sep 25, 38; E-Health Insider 2004 Mar 10

Canada

Canada does not have, currently, a national health service recipient unique identifier. Over the years, extensive work has been undertaken on this matter. In 1987, the Report of the Standing Committee on Justice and of the Solicitor General⁷⁹ made strong recommendations on the need to contain the use of the Canadian social insurance number and, in response, the Federal Government indicated that it would act to ensure that the SIN did not become a universal identification number.

The Canadian Institute for Health Information (CIHI) Working Group on Health Identification Systems has explored the current state and future plans for unique identifiers. The key points of relevance were: a wide variety of unique identifiers were found to be in use in the Canadian healthcare system with varying levels of sophistication.⁸⁰

Canada Health *Infoway* has focused on client registries as its solution to unique identification of patients for electronic health record purposes. Infoway defines a client registry as “like a ‘white pages’ phone book, a directory of people being treated”.⁸¹ The client registry “uniquely identifies individuals across a large segment of a regional healthcare continuum, typically an entire jurisdiction” and will serve as a “single ‘source of truth’ in each jurisdiction”.⁸² As defined by Infoway in 2005, the client registries will include a range of identifying data about all people who have received healthcare in a given jurisdiction: static “natural person” identifying information (such as birthdate), dynamic natural person identifying information (such as address and telephone number), and static and dynamic “artificial person” identifying information (such as various health identifiers used by individual providers) Jurisdictional client registries will recognize that individual clients may have multiple health identifier numbers even within a single jurisdiction, and will provide identification services to enable unique identification of individuals for electronic health record purposes despite the existence of those multiple identification numbers.

EU Level

At EU level, since 1990, the European Commission (EC) has been very active in designing systems for unique patient identification. The European approach is centred on smart card technology. These activities were conducted in cooperation with the European Committee for Standardization (CEN). The analysis conducted by ten working groups of the EUROCARDS action showed that many European countries are considering the development of smart cards for their health care system. Such a card was not seen as a stand-alone element, but as a key component of an integrated health information system. Issues of confidentiality and security emerged as major concerns. Equally, there was consensus that the decision to use a card containing personal medical information should remain with the person on a voluntary basis.

In a Commission document published in 2004, it was stated that-

⁷⁹ *A Review of the Access to Information Act and the Privacy Act (1987)*

⁸⁰ One of the papers produced was *National Unique Provider Identifiers A Background Paper Unique Identifiers in Health (September 2000)*

⁸¹ Canada Health Infoway 2004

⁸² Canada Health Infoway 2003

“the need to identify a person unambiguously is an important component of the interoperability of health information systems. The *eEurope2005* action plan already supports the development of standards for a common approach to patient identifiers and electronic health record architecture. The new European Health Insurance Card⁵⁵ includes a patient’s personal identification number as part of the data allowing people to use the card to get treatment outside their home Member State.”

It added, that by end 2006, “Member States, in collaboration with the European Commission, should identify a common approach to patient identifiers. This should take account of best practices and developments in areas such as the European Health Insurance Card and identity management for European citizens.”

APPENDIX 3: NATIONAL POPULATION HEALTH REGISTRIES

The aim of national population health registry or database for a particular category of disease or illness is to:

- achieve 100 percent capture of cases (100% ascertainment),
- minimise case duplication, and
- be aware of major events, such as the death of a patient,

with a view to providing a repository of information for healthcare planning and research that ultimately benefits the patient suffering from the illness or disease.

To date, in Ireland, the question of establishing national healthcare registries based on personal information has been on an ad hoc basis as with the National Cancer Registry (NCR) and the Health (Provision of Information) Act 1997. The background was that, having accepted the medical evidence that the time was right to proceed with national screening programmes for breast and cervical cancer, there was a need to populate the required registers in a manner consistent with data protection law. To operate effectively, both programmes required up- to-date population registers containing names and addresses of women in the target age group, so that they could be invited for screening.⁸³ The women's details would be retained on the registers until they moved outside the target age group.

The NCR is subject to data protection law in how the information is managed, stored and used and the National Cancer Registry of Ireland sets out its legal and moral position on preserving confidentiality very clearly.⁸⁴

The Data Protection Commissioner 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.”⁸⁵

Other Countries

Canada

Canada has a well developed system of health registries and databases that capture information across the continuum of health care services in Canada. The Canadian Institute for Health Information⁸⁶ (CIHI) which is a federally chartered, independent organization is responsible for most of these databases and registries: namely-

⁸³ The intention was that women would be invited to attend for screening as soon as they reached the appropriate age and, therefore, that the registers would need to be updated constantly.

⁸⁴ See www.ncri.ie for the full statement on confidentiality and the treatment of personal health information by the NCRI.

⁸⁵ Annual Report of the Data Protection Commissioner for 1997, page 32.

⁸⁶ All CIHI's data holdings are subject to strict privacy and confidentiality principles set out in CIHI Principles and Policies for the Protection of Health Information.

- [Canadian Joint Replacement Register](#) (CJRR)
- [Canadian Medication Incident Reporting and Prevention System](#) (CMIRPS)
- [Canadian Organ Replacement Register](#) (CORR)
- [Continuing Care Reporting System](#) (CCRS)
- [Discharge Abstract Database](#) (DAD)
- [Home Care Reporting System](#) (HCRS)
- [Hospital Mental Health Database](#) (HMHDB)
- [Hospital Morbidity Database](#) (HMDB)
- [National Ambulatory Care Reporting System](#) (NACRS)
- [National Rehabilitation Reporting System](#) (NRS)
- [National Prescription Drug Utilization Information System](#) (NPDUIS)
- [National Trauma Registry](#) (NTR)
- [OECD Health Database \(Canadian Segment\)](#) (OECD)
- [Ontario Mental Health Reporting System](#)
- [Ontario Trauma Registry](#) (OTR)
- [Therapeutic Abortions Database](#) (TADB)

To protect privacy, only a limited number of CIHI analysts have access to each data holding and their access rights are reviewed regularly. CIHI also has tools in place that can mask specific data elements from analysts. Reports and publications based on the data are subject to controls and procedures to minimize the risk of possible re-identification of an individual. CIHI discloses limited data to external researchers, who are usually associated with academic institutions or organizations. In these cases, consistent with CIHI policy (except where patient consent to release identifiable information is obtained), the data are de-identified before the disclosure.

Not all the Registries benefit from mandatory disclosure provisions. CIHI has stated that the experience with consent has been mixed and in some cases: for example, the Organ Replacement Registry, the non-consent rate had the potential to seriously affect the value of the data holding.

England and Wales (but not the rest of the UK)

Essentially, section 60 of the Health and Social Care Act 2001 grants the Secretary of State for Health powers to determine how patient data can be used in the NHS. In exercising his or her powers, the Secretary of State must comply with the requirements of the Data Protection and Human Rights Acts. Section 60 includes a process that permits application for patient data to be used without consent, under particular circumstances. Section 61 of the Act prescribed that an expert Patient Information Advisory Group (PIAG), be set up to advise the Secretary of State and the Department of Health on applications under Section 60.

In England and Wales, the Health Service (Control of Patient Information) Regulations 2002⁸⁷ (made under the Health and Social Care Act 2001) allow for the creation of a cancer registry.⁸⁸ Regulation 2 allows, subject to approval by the Secretary of State for Health, the processing of patient information in connection with the construction and maintenance of databases by bodies (known as "cancer registries") which undertake the surveillance of health and disease of patients referred for the diagnosis or treatment of neoplasia. Regulation 4 provides that information may be processed in accordance with the Regulations notwithstanding any common law obligation of confidence.

⁸⁷ Statutory Instrument 2002 (No. 1438)

⁸⁸ These Regulations are also important for research using NHS patient data.

APPENDIX 4: USING PERSONAL HEALTH INFORMATION FOR RESEARCH

Medical research is important to advances in healthcare which benefit the population as a whole, or those parts of the population with particular illnesses or conditions. This frequently requires the use of identifiable individuals' health information. As with the management of the health service, reconciling the rights of individual to control the use of their information with the greater good to the community that can come from research presents a challenge.

National Health Research Strategy

There has been a national strategy for health research – *Making Knowledge Work for Health: A Strategy for Health Research* – in place since 2001.⁸⁹ The Strategy reflects the view that knowledge-based innovation and new ways of thinking are required for the future development of the health services. 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 overlap between the fair processing requirements of the Data Protection Acts and the consent requirements of the common law means that a data controller proposing to disclose personal health information to a third party researcher should obtain the explicit consent of the patients involved, not just to ensure that the release is fair and lawful, but to guard against potential patient complaints and legal actions over inappropriate disclosure.

It is argued by some engaged in research that, while consent is a valid general principle, there are several reasons why it may not be reasonably practicable to gain individual patient consent in certain cases. These include where disproportionate or prohibitive effort or cost is required (for example, research involving thousands of historical records) or because the sensitivity of much needed research is likely to see consent withheld (for example, studies into domestic violence). More generally, it is sometimes argued that the very fact of having to ask individuals about using their information for a particular research project is likely to make them refuse. However, the Canadian Privacy Commissioner rejected this view based on a survey carried out by the Canadian Medical Association.⁹⁰

Health Research, Data Protection & the National Health Information Strategy

The Health Information Strategy identified health research as an area that needed facilitating and commented that “it is essential that there is a robust legislative basis to support appropriate research activities, together with inbuilt safeguards to protect privacy and confidentiality”.

⁸⁹ Department of Health and Children (2001)

⁹⁰ Privacy Commissioner (Canada) (2000).

Data Protection Acts and Health Information Kept for Statistical or Research Purposes

Personal information kept for research purposes is fully within the scope of the Data Protection Acts and must meet all the relevant data protection principles subject only to any clear and specific exceptions set out in the legislation. However, there are certain exemption provisions in the Acts relating to research which are designed to facilitate genuine study and scholarship by a data controller while at the same time protecting the rights of the individual, especially as regards any harm that he or she might potentially suffer from such studies. But these exemptions do not cover the situation where information is intended to be released to a third party for research purposes, for example by a doctor to a university.

In November 2007 –after a consultation exercise- the Commissioner issued ***Data Protection Guidelines on Research in the Health Sector*** which emphasized the need for patient consent to disclosure where third party research is involved.⁹¹ (The Guidelines Paper also looked briefly at Population Health Registries, Electronic Health Records system and Clinical Audit. Legislation is recommended for the creation of the Registries. The ongoing work of the EU Article 29 Group is cited as relevant to EHR systems. For clinical audit, implied consent is indicated as appropriate where the work will benefit the patient directly or where the audit is carried out by the facility treating the patient while informed consent is required in cases of third party audit.)

Research Ethics Committees

A somewhat separate but nonetheless important aspect of proper research governance concerns the role of Research Ethics Committees. In contrast with other countries around Europe, Ireland does not have an overall framework within which ethics committees operate. Some developments, however, have taken place in Ireland in recent years including the setting up of the Irish Council of Bioethics and the transposition of the EU Directive on Clinical Trials on Medicinal Products for Human Use Regulations 2004.

Issues dealt with in these Regulations include:

- procedures for obtaining a favourable ethics committee opinion (a single ethics committee opinion is required in the case of multi-centre trials);
- procedures for obtaining authorisations for the conduct of clinical trials from the Irish Medicines Board;
- controls that are to apply to the manufacture, supply and importation of investigational medicinal products;
- obligations for the reporting of various adverse events encountered in subjects participating in clinical trials, including the recording, reporting and notifying of such events;

⁹¹ Available on the website of the Data Protection Commissioner (www.dataprivacy.ie)

- obligations for compliance with standards of good clinical practice (GCP) and good manufacturing practice (GMP).

There are thirteen Research Ethics Committees currently recognised by the Department of Health and Children for the purposes of providing ethical review for clinical trials. However, clinical trials account for a relatively small number of studies taking place in Ireland and in the absence of a national structure for ethics review there are a number of difficulties arising. Specifically, where a study takes place in a number of settings or across different institutions, researchers may have to seek ethical review from several research ethics committees. In addition, there may be some difficulties arising in respect of the expertise of REC members to review certain types of research including, for example, qualitative research or social sciences.

The Office of the Minister for Children has recently commissioned a study on the operation of research ethics committees in Ireland and it is expected that this work will be completed by early 2009. In addition, a report on the structure and organisation of research ethics committees within the Health Services Executive (HSE) with recommendations for future developments has recently been completed.

Other Countries

It is useful to consider the position in other countries.

England, Wales, Scotland and Northern Ireland

Data protection legislation in the United Kingdom is based on the same EU Directive as our Acts and common law obligations on confidentiality of medical information are similar. It is, therefore, informative to see how the issues of using personal health information for research have been addressed in that jurisdiction and, in particular, the differences within different constituent elements of the UK.

The first point is confusion between the extent to which data protection legislation actually affected the existing common law position. This was the subject, in 2001, of conflicting views between a government Minister and the Information (Data Protection Commissioner) after an article appeared in the London Times (by Professor Julian Peto) headed “Data law is a killer”.⁹² The Minister stated

“..data can be used for any medical research purpose under the [Data Protection] Act without the need for consent of individuals.....Where there are problems for medical researchers, they relate to the common law duty of confidence, not data protection legislation. The effect of the common law of confidence is that patients’ consent to the disclosure of their medical data is required unless there is an overriding public interest.”⁹³

The Information Commissioner then wrote that the law of confidence while certainly relevant, as the Minister asserted, but so too is the data protection law: “...it is the meeting of the data protection principles with the duty of confidence that makes

⁹² The Times (15 May 2001) “*Privacy Law & Medical Research*”.

⁹³ The Times (Lord Falconer) (17 May 2001)

consent so integral to using and disclosing personal health information fairly and lawfully”.

In England & Wales, the government has made it clear that informed consent is the fundamental principle governing the use of patient identifiable information by any part of the NHS or research community.⁹⁴ Notwithstanding this, the matter of bypassing, or overriding, consent for management and research purposes (whether arising from the common law or data protection law) has been dealt with through section 60 of the Health & Social Care Act 2001 (already referred to as relevant to population registers). The section gives the Secretary of State for Health power to ensure that patient-identifiable information needed to support essential NHS activity can be used without the consent of patients. The power can only be used to support medical purposes that are in the interests of patients or the wider public, where consent is not a practicable alternative and where anonymised information will not suffice. The provision has been asserted to be a transitional measure, while consent or anonymisation procedures are developed.

The Section 60 arrangement has generated considerable criticism⁹⁵ and was rejected in Scotland after a major study⁹⁶ which concluded legislation of this type:

“... will restrict in particular circumstances an individual’s right to privacy. This might have the effect of causing patients to lose faith in NHS Scotland and to withhold information because of concerns that their confidentiality might be breached.....”

In Northern Ireland, the Department of Health, Social Services & Public Safety issued a consultation paper in June 2002 entitled *Health & Personal Social Services: Protecting Personal Information*.⁹⁷ In the responses published in March 2003, the Department stated:

“There was no consensus on the question of whether legislation similar to section 60 of the Health & Social Care Act 2001 to override the duty of confidence should be introduced, and if so, whether it should be permanent or temporary.”⁹⁸

Canada

In both Canada and Australia, the Federal nature of the countries make the research situation potentially very complex especially where a project covers more than one Province or State and competing considerations of National and Provincial/State rules apply. This consideration of the research rules in Canada and Australia will concentrate on the national law.

⁹⁴ Department of Health (UK) (2001)

⁹⁵ See for example, the BMJ article in 2001 claiming that the measure upset the established balance between patient privacy, professional autonomy, public health effectiveness, and the needs of scientific research. (<http://bmj.bmjournals.com/cgi/content/full/328/7447/1029#REF3#REF3>)

⁹⁶ Confidentiality & Security Advisory Group for Scotland (2002).

⁹⁷ Department of Health, Social Services & Public Safety (Northern Ireland) (2002).

⁹⁸ Department of Health, Social Services & Public Safety (Northern Ireland) (2003).

Section 7 of the Canadian Federal Personal Information Protection and Electronic Documents Act exempts organisations from seeking consent for the disclosure and use of information for certain purposes, one of which is scholarly research. Specifically, the Act permits an organisation to use or disclose personal information without the knowledge or consent of the individual to whom it pertains, if each of the following five conditions is met:

- ◆ the disclosure or use must be strictly for statistical or scholarly study or research,
- ◆ the purposes cannot be achieved without using or disclosing the information,
- ◆ the information must be used in a manner that safeguards its confidentiality,
- ◆ obtaining consent must be impracticable,
- ◆ the organisation or party seeking exemption under section 7 must inform the Privacy Commissioner of the proposed use or disclosure beforehand.

The Canadian Privacy Commissioner stated in his 2001 *Annual Report* that he intended to interpret very broadly the definition of statistical or scholarly study in the Act and to take an expansive and liberal view on the question of impracticability of consent. However, he made clear that this liberal interpretation was balanced by:

“... an absolutely inflexible requirement: the information used for health research must remain strictly within the confines of the research project and it must be used in a manner that cannot in any way harm the individual to whom it pertains.”⁹⁹

Australia

Under the Information Principles set out in the Privacy Act, agencies are not permitted to use or disclose in identifiable form records of personal information for research and statistical purposes, unless specifically authorised or required by another law, or the individual has consented to the use or disclosure. However, section 95 of the Privacy Act provides a process –the issue of guidelines by the National Health and Medical Research Council (NHMRC)¹⁰⁰ with the approval of the Privacy Commissioner- to resolve the conflict that may arise between the public and private interest in privacy and the public interest in medical research, where medical research using personal information held by a Commonwealth agency would otherwise involve a breach of privacy under the Privacy Act. The Commissioner may only approve the guidelines if satisfied that the public interest in the promotion of research of the kind to which the guidelines relate outweighs to a substantial degree the public interest in maintaining adherence to the Information Principles.

The section 95 guidelines, now in operation, 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 guidelines. The guidelines 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.

⁹⁹ Privacy in Health Research: Sharing perspectives and Paving the Way Forward: Radwanski, G. (2002)

¹⁰⁰ The Guidelines can be viewed at www.mhmrc.gov.au/publications

The Privacy Amendment (Private Sector) Act 2000 provides protection of personal information held by organizations in the private sector and section 95A Guidelines apply to such organizations.

Separate from the Guidelines, collection of health information for research purposes may also be authorized for health purposes where (a) it is impracticable to seek consent from the individual(s) involved, (b) it is authorised under a specific law or (c) is in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.