Department of Health and Aged Care

Acute and Coordinated Care Branch

Consumer Consent in Electronic Health Data Exchange

Background Paper

Final Version

1 December 2002

Roger Clarke

Xamax Consultancy Pty Ltd

Consumer Consent in
Electronic Health Data Exchange

Background Paper

EXECUTIVE SUMMARY

1. Introduction

The Acute and Coordinated Care Branch (ACCB) is responsible for a comprehensive program of Coordinated Care Trials. Many of these involve new uses and disclosures of patient data. Moreover, many of them involve, or soon will involve, electronic transmission of patient data. Consideration therefore needs to be given to the need for, and implementation approaches to, electronic forms of patient consent, referred to in this document as 'e-consent'. Further background is provided in section 1 of the body of this document.

The primary objective of the e-Consent Project is to identify practicable models whereby patient consent can be expressed and communicated in electronic contexts (section 2). It is intended that conceptual models be produced that are rich enough to reflect the diverse array of circumstances that arise in coordinated care. Building on these models, candidate technologies can be evaluated, guidelines and specifications prepared, and prototypes commissioned.

2. Underlying Concepts

If the challenges are to be successfully addressed, a number of underlying concepts need to be understood, their implications thought through, and the resulting appreciation embodied in the new initiatives.

Two critical notions are confidentiality (addressed in section 3.1 of the main report), and the multiple dimensions of privacy (3.2). **Confidentiality** is a branch of the law, which imposes obligations on natural and legal persons in relation to the disclosure of information.

Privacy is of more recent origin, more complex and more fluid. It is the interest that individuals have in sustaining a 'personal space'. Of particular relevance is the dimension of 'information privacy', which is the interest individuals have in exercising control over information about themselves. Information privacy is seriously challenged by health care practices, particularly in a coordinated care setting.
A further cluster of important concepts that need to be embodied in models for e-consent relate to the identification of patients and carers. **Identification** refers to the process of associating data with a person (4.1). Closely associated with identification are

the concepts of digital personae, roles and agents. A transaction that is conducted without identity is **anonymous** (4.2). An intermediate concept exists, which involves indirect identification of the person, by means of a **pseudonym**, which is subject to some form(s) of protection against disclosure of the relationship between pseudonym and identity (4.3). **Authentication** is the process of establishing a degree of confidence in some assertion (4.4). One form of assertion that is often the subject of authentication is that a person is who they purport to be, but other forms of authentication are also important in health care settings.

All of these concepts are used in conventional health care, and need to be applied in new settings and in electronic communications relating to health care. Of especial concern is that patients and carers who are **persons at risk** (4.5) have anonymity and pseudonymity available to them in a manner that protects them against those risks. This creates discomfort for health carers and administrators who have a pre-disposition to have access to all data about every patient, on the assumption that any data may be relevant to diagnosis, care or administration.

The Principles established under general privacy laws make consent central to the use and disclosure of patient data. The concept of **consent** (section 5.1) involves a person concurring with some other person's proposed action or opinion. It has an emergent meaning under general privacy laws (5.2). It also has specific meanings in health care law, policy and practice. Some of these arise in the context of privacy of the person (6.2), others in the context of information privacy (6.3), and yet others under health-specific data privacy laws (6.4).

A considerable body of law relates to the **capacity** of a person to provide consent (6.5). A number of other **characteristics** of consent are important (6.6), including:

- the extent to which consent is express, implied or inferred;
- whether consent may be presumed, but denied;
- the extent to which consent and denial may be over-ridden;
- the extent to which consent is informed;
- the extent to which consent is freely-given;
- the specificity and boundedness of consent;
- the extent to which consent may be varied and revoked;
- the nature and process of delegation of consent.

3. A Framework for e-Consent

A framework is proposed that enables the models for e-consent to be developed. This commences with a discussion of the recently-emerged concepts of 'opt-in' and 'opt-out' (7.1). A set of forms of consent is then proposed, including the kinds of circumstances to which they are applicable (7.2). These range from no consent, through various kinds of inferral and implication of consent, to explicit consent. Explicit consent is variously general or specific, may or may not be formally signified, and may be exercised by means of the data subject exercising control over the data.

This is followed by assessments of stakeholder categories (7.3), circumstances of use (7.4), possible implementation mechanisms (7.5), technical infrastructures (7.6) and organisational infrastructures (7.7).

4. Alternative Models for e-Consent

The framework is then used to derive a set of alternative models whereby e-consent could be implemented. One extreme is a paternalistic, non-consensual model that would be highly permissive, and hence convenient for health care professionals. The other is a purely consent-based model, which would be inconvenient for health care professionals and harmful to the quality of care they provide.

Between the two extremes, several models are outlined, which offer various balances between the two sets of interests.

Consumer Consent in Electronic Health Data Exchange
Background Paper

CONTENTS

Department of Health and Aged Care
Acute and Coordinated Care Branch

Consumer Consent in Electronic Health Data Exchange

Background Paper
Final Version of 1 December 2002

Roger Clarke

1. BACKGROUND

The Acute and Coordinated Care Branch (ACCB) is responsible for a comprehensive program of Coordinated Care Trials. Many of these necessarily involve sharing of patient data among multiple health care providers and groups. Electronic communications are increasingly being used to transmit that data. The new context creates many new opportunities for enhanced services and improved resource-efficiencies; but it also creates new threats to the confidentiality of patient data, and hence public concerns. In particular, issues arise relating to confidentiality, access authorisation, and patient consent.

In order to facilitate the application of electronic tools in support of coordinated care, consideration is being given to ways in which health care consumers can be involved in decisions about access to data about themselves. The term 'e-consent' has been coined to express the central concept. In order to flesh out this notion, conceptual models need to be explored, candidate technologies identified and evaluated, and practices defined whereby those technologies can be deployed.

The purpose of this document is to provide background to the initiative, and to the challenges it is confronting. It works towards definition of the dimensions of the problem, and of the factors that require consideration in formulating solutions. It is intended that it provide a basis for discussions with a Core Reference Group. Subsequent work would be required to define various models that are appropriate to particular categories of circumstances. In the event that the initiative gains support from the Reference Group, it would then be necessary to devise field trials that would test the models, technologies and practices, and then to prioritise and commission pilots.

2. OBJECTIVES

The primary objective of the e-Consent Project is to identify practicable models whereby patient consent can be expressed and communicated in electronic contexts.

The priority areas of application are those that support coordinated health care. This is typified by data-sharing among multiple teams of health care professionals and institutions, and uses and disclosures of patient data that are additional to those that have hitherto occurred.

More specifically, the aims are:

- to identity and trial effective mechanims for health care consumers to maintain control over new forms of access to information about themselves;
- to ensure that appropriate health care consumer authorisation is recognised and obtained in any access to patient information, which would not normally be accessible to a practitioner;
- to ensure that new technology does not undermine existing levels of control that consumers exercise over information about their health, for example by purposefully attending different practitioners for different problems.

The outcomes of the complete e-Consent Project are intended to include:

- a set of conceptual models that are capable of being implemented in order to address the full range of needs;
- a set of candidate technologies that have been identified as having potential to contribute to solutions;
- specifications of the requirements of technological infrastructure to support the various models;
- specifications of the requirements of organisational arrangements to support them;
- a set of practice guidelines to accompany technologies; and
- prototypes that have been demonstrated to be effective in particular settings.

Fulfilling that objective will ensure that patients, health care professionals and health care organisations will have good reason to develop trust in the electronic transmission of patient data. That can be expected to remove impediments to the adoption of schemes that involve electronic transmission, and hence will enable enhancements to services, and to the effectiveness and efficiency of services.

A wide range of factors act as constraints on the primary objective. There are many circumstances in which legal authority exists for a person or organisation to divulge patient data without consent. In some circumstances, the acquisition of patient consent may be impossible, very difficult, or very expensive; or may result in significant delays. There are also practic and technical factors that may make either the signification of consent, or the transmission of that signification, difficult to effect. This paper seeks to identify and reflect such constraints.

3. CONFIDENTIALITY AND PRIVACY

The following sub-sections provide background to two concepts that underlie the question of consent.

3.1 Confidentiality

The term 'confidential' is subject to a great deal of misunderstanding and mis-use. It is very often used in a manner that is essentially empty, e.g. "we treat your information as confidential", when it is actually disclosed under a great variety of circumstances. To avoid misleading patients, the term 'confidential' should be avoided, and instead information should be provided about the circumstances in which personal data is used and disclosed.

The term 'confidential' should only be used in the context of the law of confidence. This requires any person who receives information in confidence to respect the wishes of the person who provided it to them. 'Confidentiality', when used correctly, refers to the legal duty of individuals who come into the possession of information about others, especially in the course of particular kinds of relationships with them.

Confidentiality is subject to limitations, which vary considerably depending on the circumstances. One of the contexts in which the law of confidence is well-developed is health care. No comprehensive but accessible summary of the law of confidence as it relates to health care has been identified as yet.

Laws in various jurisdictions require that some kinds of confidence be breached, such as information about child abuse needing to be reported by medical practitioners, notwithstanding the obligation of confidentiality. In some circumstances, breaching the confidence may not be an absolute requirement, but a person who reasonably exercises a judgement that it ought to, in the circumstances, be breached, may be protected against an action for breach of confidence.

In addition, a recipient of confidential information may seek the consent of the provider to pass the information on to particular people or organisations, and/or for particular purposes.

3.2 Privacy

The law of confidence is quite narrow, fairly specific, and of long standing.

During the second half of the 20^{th} century, the concept of privacy has emerged, and has increasingly been the subject of legal obligations. The concept of privacy is most usefully understood as follows:

> ***Privacy*** *is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations.*

Privacy is not a single interest, but rather has several dimensions:

- **privacy of the person**, sometimes referred to as 'bodily privacy' This is concerned with the integrity of the individual's body. Issues include compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilisation;
- **privacy of personal behaviour**. This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes much of what is sometimes referred to as 'media privacy';
- **privacy of personal communications**. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'; and
- **privacy of personal data**. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' or 'information privacy'.

An important implication of the definition of privacy as an interest is that it has to be balanced against many other, often competing, interests. In particular:

- the privacy interests of one person or category of people may conflict with some other interest of their own, and the two may have to be traded off (e.g. privacy against access to credit, or quality of health care);
- the privacy interest of one person or category of people may conflict with the privacy interests of another person, or another category of people (e.g. health care information that is relevant to multiple members of a family); and
- the privacy interest of one person or category of people may conflict with other interests of another person, category of people, organisation, or society as a whole (e.g. creditors, an insurer, and protection of the public against serious diseases).

Hence:

> ***Privacy Protection*** *is a process of finding appropriate balances between privacy and multiple competing interests.*

Data varies in **sensitivity**. It would be simple if some items of data were always sensitive, and others were not; but that is simply not the nature of the matter.

Many people have particular sensitivity in relation to;

- matters that attract the opprobrium of at least some proportion of the population (e.g. episodes like participation in de-toxification programmes; conditions like STDs; and procedures like abortion);

- matters that are values-related, and can attract the opprobrium of a patient's family (e.g. events such as a prescription for the pill);
- matters that are the subject of considerable public uncertainty or ignorance (e.g. episiodes like psychiatric counselling; conditions such as diabetes, epilepsy and spina bifida; and medications like Valium); and
- matters that are a source of embarrassment (e.g. medications like Viagra).

But even seemingly less sensitive data are causes of considerable concern to a proportion of the population, at least at particular times in their lives, or in particular contexts. For example, some people are highly sensitive about their birth-year (e.g. some people who are significantly older/younger than their spouse); and some are especially concerned about their contact details, because of the risk of being found by people who may do them harm.

All data arising in health care contexts needs to be treated with care; but some requires even greater protections.

4. IDENTIFICATION AND RELATED CONCEPTS

This section examines important concepts that underlie consent. It commences with the cluster of concepts relating to identification, including identifiers, digital personae, roles and agents. It then considers anonymity, pseudonymity and nyms. Authentication is discussed, including authentication of identity and of agency relationships. Finally, the need for care to be taken in the case of persons-at-risk is discussed.

4.1 Identification

Identification is a process whereby a real-world entity is recognised, and its 'identity' established. The notion of an **identifier** is operationalised in the abstract world of information systems as a set of information about an entity that reliably differentiates it from other, similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or may be a compound of such data as given and family name, date-of-birth and postcode of residence. An organisation's identification process comprises the acquisition of the relevant identifying information.

Contrary to the presumptions made in many information systems, an entity does not necessarily have a single identifier, but may have **multiple identifiers**. For example, a company may have many business units, divisions, branches, trading-names, trademarks and brandnames. And most people are known by different names in different contexts.

A variety of types of identifer are available, which can assist in associating data with them. Important examples are:

- **names** – or what the person is called by other people;
- **codes** – or what the person is called by an organisation;
- **knowledge** – or what the person knows;
- **tokens** – or what the person has;
- **biometrics** – or what the person is, does, or looks like.

An identifier is used by an organisation as a means of associating data with the appropriate entity (in this case, patient and employee are the most common kinds of entities). It is important to appreciate that the data held is not the entity itself, but is only a limited representation of the entity. The term **digital persona** is useful as a means of signifying a group of data items that together form a simplified representation of an entity.

Entities in general, and people in particular, perform multiple **roles**. For example, on any one day, a person may act as their private selves, as an employee of an organisation, as an officer of a professional association, and as an officer of a community organisation. In addition, a person may have multiple organisational roles (e.g. substantive position, acting position, various roles on projects and cross-organisational committees, bank signatory, first-aid officer and fire warden), and multiple personal roles (e.g. parent, child, spouse, scoutmaster, sporting team-coach, participant in professional and community committees, writer of letters-to-the-newspaper-editor, chess-player, and participant in newsgroups, e-lists, chat-channels).

One relevant use of the role concept is in recognising that health carers are also patients. Moreover, a patient may have other roles in relation to health care, such as office-bearer in a fund-raising organisation and/or in an organisation opposed to particular kinds of contentious procedures, such as abortion. In general, the digital personas representing different roles need to be kept separately and not inter-related, e.g. personnel databases are distinct from health care records.

The concept of role is also relevant to the provision of patient data in health care contexts. Some consents may be given by pat in relation to identified individuals ("yes, doctor, please send those details to Dr Buchanan"). In other circumstances, the consent is for communication of data to a role ("yes, doctor, please have a path' test done on those samples"). This highlights the fact that multiple individuals may perform particular roles at different times, e.g. because of the need for shift-work in both intensive-care and extensive-care.

A further factor that needs to be borne in mind is that one entity may act on behalf of another. Power of attorney formally attests to this relationship, but in many circumstances an **agent** may have authority under law, as is the case with parents and guardians, variously of minors and of people who are not psychologically competent to manage their own affairs.

4.2 Anonymity

At the other extremity from identification is anonymity. This arises where data cannot be associated with a particular entity, either from the data itself, or by combining the transaction with other data.

A great many transactions that people undertake are anonymous, including:

- barter transactions;
- visits to enquiry counters in government agencies and shops;
- telephone enquiries;
- cash transactions such as the myriad daily payments for inexpensive goods and services, gambling and road-tolls;
- the casting of votes in a secret ballot; and
- treatment at discreet clinics, particularly for sexually transmitted diseases.

Some of the reasons that people use anonymity are of dubious social value, such as avoiding detection of their whereabouts in order to escape responsibilities. Other reasons are of arguably significant social value, such as avoiding physical harm, enabling 'whistle-blowing', avoiding unwanted and unjustified public exposure, and keeping personal data out of the hands of intrusive marketers and government agencies.

Health care professionals have tended to deny patients the opportunity for anonymity. It does have important applications, however. Where patient data is made available to researchers for cross-sectional analysis, and no convincing case can be made for long-term retention of the data, or for association of new data with old data (as is needed in longitudinal surveys), the data must, under privacy law, be de-identified, i.e. anonymised.

4.3 Pseudonymity

Between anonymity and identification, an additional alternative exists. Pseudonymity arises where a record or transaction cannot, in the normal course of events, be associated with a particular individual. The data may, however, be indirectly associated with the person if particular procedures are followed, e.g. the issuing of a search warrant authorising access to an otherwise closed index.

Authors, actors and entertainers use nyms. So do workers in the sex industry. So do criminals (in the form of aliases and aka's). So do call-centre staff in marketing and customer service roles, in order to protect their social selves from the people that they deal with in their work-roles. The many categories of persons-at-risk discussed in section 4.5 below have especially important needs for pseudonyms.

To be effective, pseudonymous mechanisms must involve **legal, organisational and technical protections**, such that the link can only be made (e.g. the index can only be accessed) under appropriate circumstances.

Pseudonymity is used in some situations to enable conflicting interests to be satisfied; for example in collections of highly sensitive personal data such as that used in research into HIV/AIDS transmission. It is capable of being applied in a great many more situations than it is at present.

Pseudonymity can be valuably applied to reflect the various **roles** that people play. For example, where patient data is made available to researchers for longitudinal analysis, and association of new data with old data is important, the data must, under privacy law, be pseudo-identified, such that the researcher is unable to know the identifier actually associated with the data.

The term '**nym**' is useful to refer to a data-item or group of data-items that reliably distinguishes a role, rather than a specific identity.

4.4 Authentication

Authentication is the process whereby a degree of confidence is established about the truth of an assertion.

Organisations undertake **authentication of value** by checking a banknote for forgery-resistant features like metal wires or holograms, and seeking pre-authorisation of credit-card payments.

Another approach is the **authentication of attributes or eligibility**. This is commonly performed by checking some form of credential, such as a membership card, e.g. health care organisations may request a person's Medicare Number and/or private health insurance details. In this case, it is not the person's identity that is in focus, but rather the capacity of that person to perform some function or receive some benefit, such as being granted a discount applicable only to tradesmen or club-members, a concessional fee only available to senior citizens or school-children, entry to premises that are restricted to adults only, gratis treatment in a public hospital, or admission to private wards and nomination of a private doctor.

A particular case of concern is **authentication of agents**. It can be challenging in health care contexts to determine with reasonable confidence that a particular person has the authority to make decisions on behalf of another, e.g. in the cases of adolescents, of comatose patients, and of the deceased.

A further, emergent challenge is the authentication of powers delegated to **artificial intelligences or software agents**. This already occurs in automated telephone, fax and email response; automated re-ordering; and 'program trading'. Subject to some qualifications, legislatures and courts may be becoming willing to accept these acts as being binding on the entity concerned, at least under some circumstances. A proxy for authentication of a software agent is **authentication of the device or process** in which the agent is running. For example, a check might be performed of the identity of the chip in the remote processor against a pre-registered list, or digital signature might be used to test whether the device has used a pre-registered key to sign the message.

A further application of the idea is to the **authentication of a human or corporate identity**. This is the process whereby an organisation establishes that a party it is dealing with is:

- a previously known real-world entity (in which case it can associate transactions with an existing record in the relevant information system); or
- a previously <u>un</u>known real-world entity (in which case it may be appropriate to create a new record in the relevant information system, and perhaps also to create an organisational identifier for that party).

The nature of identity, identifiers, and identification processes is such that identity authentication is never perfect, but rather is more or less reliable. It is useful to distinguish **degrees of assurance** about identity. High-reliability authentication processes are generally costly to all parties concerned, in terms of monetary value, time, convenience and intrusiveness. Organisations select a trade-off between the various costs, reliability, and acceptability to the affected individuals.

4.5 Persons-at-Risk

Some categories of individual are in sensitive positions, at risk of undue embarrassment or physical harm. 'Persons-at-risk' are people whose safety and/or state of mind are greatly threatened by the increasing intensity of data-trails, because discovery of their location is likely to be followed by the infliction of harm, or the imposition of pressure designed to repress the person's behaviour.

Examples include:

- 'celebrities' and 'notorieties' such as entertainers and lottery-winners, politicians and other 'VIPs' (who are subject to widespread but excessive interest among sections of the media, zealous fans and other members of the public, including 'stalkers', kidnappers, blackmailers and extortionists);
- victims of domestic violence;
- people in sensitive occupations such as prison management and psychiatric health care;
- different-thinkers, eccentrics, people whose behaviour or beliefs are ideosyncratic, and people who are paranoid;
- protected witnesses;
- people under fatwa; and
- undercover law enforcement and national security operatives.

Persons-at-risk seek anonymity for many of their transactions, including health care. This is in conflict with the interests that the person has in quality health care, and with the expectations of many health care professionals. An alternative is to apply pseudonymity to the protection of persons-at-risk, by using a pseudo-identifier on files rather than the person's commonly-used name.

Persons-at-risk include health care professionals as well as patients. Staff in health care institutions (particularly in areas of sensitivity, such as psychiatric hospitals and wards, health care services in prisons, and abortion clinics) may use a nym, in order to avoid the identifier that they use in their social lives becoming known to persons who may represent threats to them.

5. THE CONCEPT OF CONSENT

This section identifies the meaning of consent, starting with dictionary definitions, and moving on to important factors that determine its meaning in the contexts relevant to the question of e-consent in health care.

5.1 Dictionary Definitions

The British Concise Oxford Dictionary:
verb (i): express willingness, agree
noun: voluntary agreement, compliance; permission

The American Websters Dictionary:
verb: 1: to give assent or approval
noun: 1: compliance in or approval of what is done or proposed by another
2: agreement as to action or opinion

The Australian Macquarie Dictionary:
verb (i): 1. to give assent; agree; comply or yield
noun: 3. assent; acquiescence; permission; compliance
4. agreement in sentiment, opinion, a course of action, etc.

On the basis of these definitions, the following appear to be the common elements:

- a person (A);
- an action or opinion proposed by another person (B);
- concurrence by A with B's proposed action or opinion.

Hence the following is suggested as a working definition of the term:

concurrence by a party with an action to be taken by another party

The basic concept appears to be generally independent of such questions as whether the concurrence is offered by A, or procured by B; whether A's agreement is spontaneous, or influenced by B; and whether or not B offers inducements of a positive or of a negative nature.

5.2 Definition Under Commonwealth Laws

Some aspects of privacy, and of consent, are subject to common law. An important example is the law of confidence, which has wide application in the context of patient data.

In addition, a number of statutes create privacy law.

The health care sector is generally subject to the Privacy Act 1988, as amended.

The original Commonwealth Privacy Act 1988 applied to public sector agencies of the Commonwealth and of the A.C.T. In the Information Privacy Principles defined in s.14, consent is the primary pre-requisite to use and to disclosure of personal data, at:
http://www.austlii.edu.au/au/legis/cth/num%5fact/pa1988108/s14.html.
(In most such sets of principles, consent is also a control governing the collection of personal data; but that is not the case with the Australian Act).

The Commonwealth Act provides no formal definition of 'consent', however.

The Privacy Act was amended with effect from December 2001, to extend its coverage to the private sector. A different set of principles applies, commonly referred to as the 'National Information Privacy Principles'. The Amendment Act established both generic laws applicable to all private sector activities including health care, and specific provisions relating to health care.

Medical research is subject to additional, more detailed guidelines under the Commonwealth Privacy Act 1988, which were defined and are maintained by the National Health & Medical Research Council.

Appendix 1A contains extracts from, and references to, those laws.

5.3 Definition Under State and Territory Laws

Some aspects of privacy, and of consent, are subject to common law within State and Territory jurisdictions. An important example is the law of confidence, which has wide application in the context of patient data.

The public sector health care sector in **N.S.W.** is subject to the N.S.W. Privacy And Personal Information Protection Act 1998, at
http://www.austlii.edu.au/au/legis/nsw/consol%5fact/papipa1998464/index.html.
In common with most other statutes, this Act provides no formal definition of the terms 'privacy' or 'consent'.

There is a considerable number of additional laws of relevance. Appendix 1B contains extracts from, and references to, many of those laws.

The **A.C.T.** Health Records (Privacy and Access) Act 1997 directly regulates health care records in both the public and private sectors. Appendix 1C contains extracts from, and references to, that law.

Victoria has a variety of longstanding laws of relevance. In addition, the Victorian Information Privacy Act 2000 now regulates the public sector in that State, and a companion statute, the Health Records Act 2001, which directly affects the health care sector as a whole, came into force on 1 July 2002. Appendix 1D contains extracts from, and references to, those laws.

6. CONSENT IN THE HEALTH CARE SECTOR

This section considers the application of the concept of consent within the specific context of the health care sector.

6.1 Consent in Health Care Contexts

In health care, consent is relevant to:

- invasions of the privacy of the person, such as surgical and other invasive procedures;
- invasions of the privacy of personal behaviour, such as observation by third parties such as medical students;
- invasions of the privacy of personal data, such as disclosure of medical records.

This project is concerned with e-consent in relation to health data exchange, and accordingly the main focus is on the third of these contexts. However there is a considerable body of law in the area of consent in relation to privacy of the person, and this is likely to be of at least some relevance to consent in relation to use and disclosure of personal data. The following section accordingly undertakes a brief review of that law.

6.2 Consent in Relation to Privacy of the Person

A variety of health-specific laws contain provisions relating to consent in relation to privacy of the person. A selection is noted here, because it provides context to the discussion that follows. Examples include:

- s.19 of the N.S.W. Human Tissue Act 1983 provides that "A person, other than a child, may consent to the **removal of blood from the person's body for the purpose of ... its transfusion to another person** ...", , at http://www.austlii.edu.au/au/legis/nsw/consol_act/hta1983160/s19.html;
- under s.9 of the A.C.T. Transplantation And Anatomy Act 1978, a person's consent is required for the "removal from his or her body, at any time after the expiration of 24 hours from the time at which the consent is given, of **specified non-regenerative tissue for the purpose of the transplantation of the tissue to the body of another living person**", at , at http://www.austlii.edu.au/au/legis/act/consol_act/taaa1978298/s9.html;
- legal authority to perform **forensic procedures** without consent are provided to magistrates under the Commonwealth Crimes Act s.23WR, at http://www.austlii.edu.au/au/legis/cth/consol%5fact/ca191482/s23wr.html, and to a senior constable, under the Commonwealth Crimes Act ss.23WN, 23WO, at http://www.austlii.edu.au/au/legis/cth/consol%5fact/ca191482/s23wn.html.

6.3 Consent in Relation to Privacy of Personal Data

Various categories of personal data arise in health care contexts. Key instances are:

- data that identifies individuals;
- data that provides contact details for individuals;
- details of:
  - a health care event;
  - a health care encounter;
  - a health care episode;
  - a health care condition;
  - a health care procedure; or
  - a medication;
- summary data relating to an event, encounter, episode, condition, procedure or medication;
- data that discloses that a record of some kind exists.

Privacy generally, and consent to use and disclosure of the data in particular, are issues in every one of these instances.

6.4 Definition of Consent Under Health-Specific Data Privacy Laws

In general, patient data held in the **public sector** is subject to laws of the applicable jurisdiction, i.e. the Commonwealth or the relevant State or Territory. These laws include various health-related statutes, general privacy laws, and disallowable instruments such as NH&MRC Guidelines and Regulations under such statutes.

Patient data held in the **private sector** is subject to general privacy laws, and in some jurisdiction also to express health care sector laws. Important among these are:

- the Commonwealth Privacy Act 1988, which has regulated the public sector since 1988, and, since the end of 2001 the private sector as well;
- the A.C.T. Health Records (Privacy and Access) Act 1997;
- the N.S.W. Privacy And Personal Information Protection Act 1998 and Health Records and Information Privacy Act 2002; and
- the Victorian Information Privacy Act 2000 and Health Records Act 2001.

Details are provided in section 5 above, and in Appendices 1A-1D.

6.5 Capacity to Give Consent

Circumstances arise in which a person is physically or legally incapable of giving consent. Many of these are subject to explicit laws, or to codes of practice.

In relation to **children**, for example:

- the Commonwealth Crimes Act 1914 s.23WE provides that a child cannot consent to forensic procedures, at: http://www.austlii.edu.au/au/legis/cth/consol%5fact/ca191482/s23we.html;
- under s.20 of the N.S.W. Human Tissue Act 1983, special provisions apply to donations of blood by children, at: http://www.austlii.edu.au/au/legis/nsw/consol_act/hta1983160/s20.html;
- the N.S.W. Children And Young Persons (Care And Protection) Act 1998 s.177 regulates consent in relation to medical and dental treatment, at: http://www.austlii.edu.au/au/legis/nsw/consol%5fact/caypapa1998442/s177.html;
- the A.C.T. Health Records (Privacy and Access) Act 1997, at s.25, vests the powers to consent to patient information access, use and disclosure in **a minor's guardian**, and not in the minor, at http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/s25.html;
- the N.S.W. Health Information Privacy Code of Practice specifies consent by the guardian up to age 14, consent by the patient if over 16, and considerable care between the ages of 14-16 (section 7.3.2, p.29);
- the N.S.W. Health Records and Information PrivacyAct 2002, at s.8, defines an **authorised representative** as being able to act for a child up to the age of 18 years.

Some **other exceptional circumstances and minority groups** for which special provisions may exist, or may be needed, include the following:

- older people;
- comatose, seriously incapacitated or frail people;
- 'street kids';
- itinerants; and
- indigenous Australians living traditional lifestyles.

Legislation varies considerably in relation to such people. For example:

- under the Commonwealth Crimes Act 1914 s.23WE, **an 'incapable person'** cannot consent to forensic procedures, at: http://www.austlii.edu.au/au/legis/cth/consol%5fact/ca191482/s23we.html;
- the N.S.W. Mental Health Act 1990 s.174 specifies procedures in relation to psychosurgery where the relevant Board is not satisfied that "the patient the subject of the application is capable of giving informed consent", at: http://www.austlii.edu.au/au/legis/nsw/consol%5fact/mha1990128/s174.html;
- the A.C.T. Health Records (Privacy and Access) Act 1997, at s.26, vests the powers to consent to patient information access, use and disclosure in the guardian of **a 'legally incompetent person'**, and not in the person themselves, at http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/s26.html.

  A 'legally incompetent person' is defined in s.4 as one in relation to whom an enduring power of attorney or guardianship order has become operative;
- the N.S.W. Health Information Privacy Code of Practice specifies consent by the guardian of **a 'patient who lacks mental capacity'** (section 7.3.4, p.29);
- the N.S.W. Health Records and Information Privacy Act 2002, at s.7, specifies that an authorised representative is to act on a person's behalf "if the individual is **incapable** (despite the provision of reasonable assistance by another person) **by**

reason of age, injury, illness, physical or mental impairment of: (a) understanding the general nature and effect of the act, or (b) communicating the individual's intentions with respect to the act"..

Generally, people make the presumption that privacy expires with a person's life. In at least some Australian jurisdictions, this is a mistaken presumption. For example:

- the A.C.T. Health Records (Privacy and Access) Act 1997, at s.27, vests the powers to consent to patient information access, use and disclosure in **the legal representative of a deceased person** (under s.4, the executor or administrator), at http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/s26.html;
- the N.S.W. Health Information Privacy Code of Practice specifies consent by **the next-of-kin, or executor or administrator** (section 7.3.5, p.29);
- under the N.S.W. Health Records and Information Privacy Act 2002, at s.5, personal information includes "information about an individual who has been dead for [less] than **30 years**".

6.6 Characteristics of Consent

This sub-section identifies the requirements that need to be satisfied for it to be reasonably claimed that the use or disclosure of patient data has been consented to.

(1) Express, Implied and Inferred Consent

By **'express consent'** is meant that the individual giving the consent provides explicit **signification** that they have granted it. Express consent may be:

- **'consent in writing'** (including other recorded form, such as an email, or a tick in a box on a web-form); or
- it may given in a manner which gives rise to **no record** (in particular, verbal or visual approval). In such cases, there are benefits in the person to whom the consent is communicated recording how consent was signified.

The notion of **'implied consent'** is conventionally used to refer to two rather different circumstances:

(1) **the individual implies consent through their behaviour**. This arises, for example, where the person provides information in a context in which it is clear that the information will be used for some purpose, or will be disclosed to some other person. This is a matter that can be subject to dispute. A record that conveys the context is of importance in determining whether consent has or has not been implied;

(2) **someone else infers that the individual gives consent**. This arises where some person claims that the context is such that consent can be assumed. This is much more usefully termed '**inferred consent**'. It is a much more contentious situation, and needs to be subjected to controls.

Under the Commonwealth Privacy Act s.6, consent may generally be express or implied: http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html#consent

In some circumstances, express consent in writing is required by law or a code of practice. For example:

- under s.7 of the A.C.T. Health Records (Privacy and Access) Act 1997, a 'health status report' may be neither collected from a person other than the patient, nor disclosed to a person other than the patient, without written consent, at http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/s7.html;
- the N.S.W. Health Information Privacy Code of Practice states that "the client/patient's authority should be in writing" (section 7.4.2.2, p.31).

Many circumstances arise in health care in which few parties would contest that 'implied consent' exists. There are also circumstances in which 'inferred consent' is reasonable.

An example of reasonably inferred consent is access to the wallet or purse of an unconscious person who has been involved in an accident and who urgently needs t a tranfusion or sedation, in order to search for any evidence of the person's blood group and any known allergies.

An example of inferred consent that is more contentious is access by an M.P. on behalf of a constituent. The N.S.W. Health Information Privacy Code of Practice states that "Members of parliament making representations on behalf of a constituent are also required to have authorisation" (section 7.4.2, p.31).

(2) Denial of Consent – Express, Implied and Inferred

Circumstances arise in which a person's consent might be inferred or assumed. For example, in many countries of Continental Europe, the law creates a presumption that a person's organs are available for transplant should they die in an accident. This presumption can be denied in advance of death by the person concerned. This is often referred to as an 'opt-out' scheme (see section 7.1 below).

Where consent is expressly denied, this needs to be recorded. For example, the N.S.W. Health Information Privacy Code of Practice states that "if consent is not given ..., this should be noted on the client/patient's health record ..." (section 6.1, p.19).

In some circumstances, denial of consent should not need to be explicit, but may be implied by the person's behaviour, or inferred from context.

(3) Informed Consent

For consent to be meaningful, the individual needs to understand the implications of the consent.

The Websters includes an entry for 'informed consent', which it places squarely within the health care sector by defining it to mean "consent to surgery by a patient or to participation in a medical experiment by a subject after achieving an understanding of what is involved". It dates the term's emergence to as late as 1967.

The Australian Privacy Charter states at:

http://www.apcc.org.au/Charter.html#PCP2
that "'consent' is meaningless if people are not given full information".

The N.S.W. Health Information Privacy Code requires (section 6.1, p.18; Appendix 3, p.55) that "There is a need for clients/patients to be better informed about how their personal health information will be used. This should include an understanding of:

- who will have access to the information;
- the reason why the information is collected;
- whether collection of the information is voluntary or mandatory (though consent will not be required if mandatory, the client should nonetheless be informed);
- how the information will be used;
- any proposed disclosure of the information to third parties; and
- if relevant, that the information will be computerised".

The U.S. Department of Health and Human Services has stipulated 'General requirements for informed consent' in the context of medical research involving human subjects. See:
http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm#46.116
This specifies over a dozen requirements, including a variety of descriptions and explanations. Although many specifically relate to privacy of the person, a number of data privacy aspects arise.

(4) Freely-Given Consent

For consent to be meaningful, there must be no duress or undue influence involved.

The Australian Privacy Charter's Consent Principle (2) states at:
http://www.apcc.org.au/Charter.html#PCP2 that "'consent' is meaningless if people ... have no option but to consent in order to obtain a benefit or service".

Further, the Charter's No Disadvantage Principle (18) at:
http://www.apcc.org.au/Charter.html#PCP18 states that "People should not ... be denied goods or services or offered them on a less preferential basis, in order to exercise their rights of privacy".

Under the A.C.T. Act s.20, "A person shall not, by any unlawful threat or intimidation, or by any false representation, require or purport to require another person ... to give a consent under this Act", at
http://www.austlii.edu.au/au/legis/act/consol%5fact/hraaa1997291/s20.html.

Under the N.S.W. Health Records and Information Privacy Act 2002, at s.70, "a person must not, by threat, intimidation or false representation, require another person … to give a consent".

S organisations seek **consent notwithstanding the existence of legal authority**; for example, the Australian Bureau of Statistics does so in respect of the census, and the small number of surveys for which participation is compulsory. This practice is contentious. The N.S.W. Health Information Privacy Code (section 6.1, p.18) states that "consent will not be required if [the data collection or disclosure is] mandatory".

(5) Specificity and Boundedness of Consent

For consent to be meaningful, it must be specific rather than vague.

In particular, it must be clear from the expression or the context:

- what **data** the consent relates to;
- what **action(s)** the consent authorises;
- to what **party or category of parties** the authorisation relates;
- for what **purpose(s)** the authorisation applies; and
- over what **time-period** it operates.

The N.S.W. Health Information Privacy Code of Practice states that "if limitations are applied, this should be noted on the client/patient's health record ..." (section 6.1, p.19). It further requires that "details of the records/information in question, and the range of dates for health treatment in question ... be in writing" (section 7.4.2.2, p.31).

(6) Variability and Revocability of Consent

Consent needs to be able to be varied at any time by the individual. It also needs to be revocable at any time by the individual. Questions arise regarding the communication of the variation or revocation, and notice required for it to take effect.

The Australian Privacy Charter states at http://www.apcc.org.au/Charter.html#PCP2 that "people have the right to withdraw their consent".

(7) Delegability of the Power to Consent

The power to consent needs to be able to be delegated to others. This is subject to a variety of laws, some general in their application (e.g. laws relating to guardianship, including persons *in loco parentis*, powers of attorney, and especially enduring / durable powers of attorney). Provisions exist in a number of health-specific laws and codes of practice.

For example, the N.S.W. Health Information Privacy Code of Practice recognises access by the patient's legal representative / solicitor, and by medical practitioners nominated by the patient (section 7.4.2.3, p.31).

7. A FRAMEWORK FOR E-CONSENT

This section presents a framework within which e-consent can be analysed. The elements of the framework are as follows:

- 'opt-in' consent versus 'opt-out' presumption of consent, complemented by denial;
- forms of consent;
- the effects of consents and denials;
- stakeholders.
- circumstances in which the question of consent arises, comprising:
  - a catalogue of circumstances;
  - characterisation of those circumstances; and
  - categorisation of the circumstances;
- implementation mechanisms for consent;
- technical infrastructure to support the mechanisms;
- organisational infrastructure to support the mechanisms.

This Background Paper does not attempt to fill out the framework, nor to apply it, but only to provide some tentative starting-points.

7.1 'Opt-In' Consent Versus 'Opt-Out' Denial

During recent years, a pair of terms has come into common usage, particularly in the context of direct marketing. The term **'opt-in'** refers to consent-based arrangements, i.e. an action may only be performed by an organisation if the person has consented to it. A consent may be express or implied, but it must be reasonably believed that it exists; otherwise the action is not permitted.

An **'opt-out**' scheme comprises the following elements:

(a) an organisation makes a **presumption of consent**, irrespective of what the person may have wished;

(b) individuals may communicate an express **denial** of their consent;

(c) the organisation takes notice of the denial.

From the privacy viewpoint, 'opt-out' arrangements are subject to a large number of **deficiencies**:

(a) they are not consent-based;

(a) there may be no mechanism whereby the individual is aware that consent has been presumed, and hence no trigger for the individual to register a denial;

(b) registering denial of consent may involve onerous actions on the part of the individual, e.g. discovering the process, making contact, acquiring forms, filling in forms, providing evidence of identity;

(c) the individual may be disadvantaged if they register a denial of consent, e.g. through withdrawal of services;

(d) the denial of consent may be ignored;

(e) the denial of consent may be treated by the organisation as having a limited scope or duration, and this might even be done where the individual expressly states a broad scope or that the denial is until further notice;

(f) there may be no recourse available should the organisation perform inappropriately, e.g. by ignoring a denial, applying penalties, or making the registration of denial onerous.

In the event that 'opt-out' presumption of consent is used in any health care contexts, care is needed in order to avoid these deficiencies.

7.2 Tentative Analysis of Forms of Consent

This sub-section considers the different forms of consent that are feasible, ranging from none, through inferred and implied, to express. Records of the assumption or authorisation may or may not exist.

(1) No Consent

There are circumstances in which:

(a) consent is not relevant; or

(b) denial of consent may be over-ridden.

Non-consensual use of data, and the over-riding of denials of consent, are extremely sensitive matters. They must not be done lightly, and they must be subject to controls.

These circumstances are of only two kinds:

- where legal authority exists; and
- emergencies (which of course occur in the health care sector much more than in any other context).

Where legal authority exists, alternative **control mechanisms** are necessary to protect the person's privacy, including:

- information for the patient when data is collected, or a relationship commences;
- recording of use or disclosure;
- recording of the legal authority invoked;
- acquisition and retention of evidence of the circumstances satisfying the legal authority; and
- information for the patient when, or after, particular use or disclosure of data occurs.

In emergencies, alternative **control mechanisms** are necessary to protect the person's privacy, including:

- information for the patient when data is collected, or a relationship commences;
- recording of use or disclosure;
- recording of, or cross-reference to, the facts of the emergency; and

- information for the patient after particular use or disclosure of data has occurred.

(2) Consent Inferred

There may be circumstances in which consent may be reasonably inferred. However, a denial of consent precludes consent being inferred.

In these cases, it is necessary to **record**:

- that consent was inferred; and
- sufficient information to enable reconstruction and evaluation, in the event that the inference in challenged.

In some circumstances, it would also be necessary to communicate to the patient afterwards that consent had been inferred. Especial care is needed in the event of any sensitivity on the part of the patient about any aspects of the use or disclosure.

(3) Consent Implied by General Context

There are many circumstances in which consent can reasonably be claimed to be implied by the context. An example is communications between a G.P. and a specialist, in relation to a patient referred from one to the other. However, a denial of consent precludes consent being claimed to be implied by general context.

Particularly where some uncertainty or sensitivity exists, it is necessary to **record** the facts that make it reasonable to claim that consent was implied, together with sufficient information to enable reconstruction and evaluation in the event that the patient disputes that consent was given. In the case of transactions with primary carers, this can be readily achieved as a by-product of treatment record-keeping.

(4) Consent Implied by Specific Context

There are many circumstances in which consent can reasonably be claimed to be implied by the specific context. However, a denial of consent precludes consent being claimed to be implied by specific context.

An example is disclosures by a treating G.P. to a pathology laboratory, where a sample of body tissue or fluids has been collected for analysis. A common and effective approach is for the patient to be informed by the health care professional as to the procedures that are being undertaken. In the event that no objection is made, consent may reasonably be claimed to be implied.

Particularly where some uncertainty or sensitivity exists, it is necessary to **record** the facts that make it reasonable to claim that consent was implied, together with sufficient information to enable reconstruction and evaluation in the event that the patient disputes that consent was given. In the case of transactions with primary carers, this can be readily achieved as a by-product of treatment record-keeping.

Examples of different kinds of contexts that may be the subject of consent, or of denials of consent, include:

- an identified health care professional;
- a particular category of health care professional;
- health care professionals in a particular location or practice;
- an event;
- an encounter;
- an episode;
- a condition;
- a procedure; and
- a medication.

(5) Consent Explicit but General

There are contexts in which consent is explicit, but expressed in general terms. An example is a consent embedded in registration for a trial. However, a specific denial of consent overrides a general consent.

In general, it is necessary to **record** explicit consents of this nature.

In addition, where reliance is placed on the general consent, sufficient information should be recorded to enable reconstruction and evaluation in the event that the patient disputes that consent was given.

(6) Consent Explicit and Specific

There are contexts in which consent is explicit, and specific as to its applicability. An example is authority to disclose particular information to a specific health or other insurance company.

A specific denial of consent overrides a specific consent, if the consent is more generally expressed. For example, the consent to pass personal data on to another doctor may be specifically qualified in respect of, for example, a particular doctor, a particular condition, or a particular episode.

In general, it is necessary to **record** explicit consents of this nature.

In some circumstances, **formal expression** of consent is appropriate, involving an action such as the provision of a written signature on a document that signifies the consent and what the consent is to (or an equivalent action, such as the affixing of the patient's

A further approach that is applicable in some circumstances is the transmission of the information from the transferor, via the patient concerned, to the transferee. An example is diagnostic results such as X-rays and ultra-sound images given to the patient for carriage back to the doctor, or given back to the patient after they have been inspected. Where **the patient exercises control over the data**, the patient is aware of, and provides clearly implied consent to, the disclosure (because the patient has the ability to preclude the data reaching the transferee).

7.3 Effects of Consents and Denials

There are several different ways in which consents and denials may be applied. The primary variations are as follows:

- **prevention or enablement of actions** based on the consent or denial, in particular the blocking of access to data, or the provision of access to data. This is referred to using various terminologies, including 'gatekeeper' mechanisms, 'access control', 'authorisations' and 'permissions';
- **real-time detection of actions** that are inconsistent with a consent or denial. This may be used to:
  - provide a warning to the person taking the action;
  - record that the action is being taken, and is inconsistent with a consent or denial;
  - notify to some appropriate person that the action is being taken, and is inconsistent with a consent or denial;
- ***ex post facto* analysis and investigation of actions** that were inconsistent with a consent or denial, in an endeavour to detect foul play, resulting in notification to some appropriate person.

7.4 Tentative Analysis of Stakeholders

The later phases of the project are dependent on participation by representatives of, and advocates for, a substantial set of individuals and organisations that have an interest in health care, and in the handling of health care information.

This is important firstly because all such stakeholders are factors in the design of e-consent mechanisms, and secondly because wide involvement should assist in devising consultative processes to accompany the development of e-consent.

7.5 Tentative Analysis of Circumstances

This sub-section proposes examination of the range of circumstances in which questions of consent may arise. It comprises the compilation of a list of circumstances, the identification of characteristics relevant to the question as to which form of consent is appropriate, followed by classification of circumstances into categories that have significant similarities.

(1) Catalogue of Circumstances

The initial phase of the project involved the preparation of a catalogue of circumstances that may involve various forms of patient consent. This was performed through a combination of literature research, workshops and discussion of exposure drafts.

Appendices are provided, which were used as the basis for the initial workshops:

- Appendix 2 provides a 'starter list' of the wide range of settings in which questions of consent may arise;
- Appendix 3 provided a 'starter list' of some specific cases, whose greater richness was intended to enable deeper analysis of the issues. That document was subsequently enhanced, and is published as a separate document in the series. Appendix 3 has accordingly been withdrawn from this final version of the Background Paper.

(2) Characterisation of Circumstances

In the next phase of the project, it was envisaged that a set of characteristics relevant to e-consent would be developed. This was to be achieved through analysis and where necessary articulation of the catalogue, supplemented by workshops and discussion of exposure drafts.

(3) Categorisation of Circumstances

Subsequently, it was envisaged that the catalogue of circumstances would be classified according to those characteristics. Once again, the primary vehicle for the development of the categorisation was envisaged to be workshops and discussion of exposure drafts.

7.6 Tentative Analysis of Implementation Mechanisms

The next phase of the project was to identify and examine practical mechanisms whereby the various forms of consent could be achieved, firstly in conventional settings, and secondly in electronic contexts. This was to be undertaken through analysis, workshops, and discussion of exposure drafts.

7.7 Tentative Analysis of Technical Infrastructure

The nature of the technical infrastructure needed to support consent was then to be examined, firstly in conventional settings, but mainly in electronic contexts. This was to be undertaken through analysis, workshops, and discussion of exposure drafts.

7.8 Tentative Analysis of Organisational Infrastructure

Organisational arrangements that are needed to support consent would then need to be examined, firstly in conventional settings, but mainly in electronic contexts. This was to be undertaken through analysis, workshops, and discussion of exposure drafts.

8. ALTERNATIVE MODELS FOR E-CONSENT

This section presents a list of possible models for e-consent. The models differ greatly in the extent to which they trade-off between the following key interests:

- of the patient:
  - in quality health care; and
  - in protection of personal data;
- of health care professionals:
  - in the accessibility of patient data; and
  - in the convenience of that access.

The first model is an entirely paternalistic approach, in which patient consent is unnecessary. This maximises access to data, and in at least a naïve sense maximises the quality of health care, in return for zero patient control over health data about themselves. A series of possible intermediate points are then traversed between that extreme and complete control by patients over data about themselves.

8.1 Irrelevance of Patient Consent

This model sees quality of care and convenience to health care professionals as paramount. Access to data is not based on consent, nor is denial of consent permitted.

The approach need not be devoid of all control. For example, each access might be conditional upon a declaration by the professional of the reason for it (e.g. a reference-identifier for the event that justifies it), logs of accesses could be maintained, automated and manual analyses of the logs could be undertaken in order to detect abnormal patterns, investigations could be undertaken, laws could specify sanctions for inappropriate access, and investigations could lead to prosecutions and civil suits.

8.2 Nominally Consent-Based, With Statutory Authorisations

An alternative model is consent-based, in that patients need to provide consent to the use and disclosure of their data. The consensual basis is, however, nominal rather than real. This can be achieved by creating an array of statutory over-rides so long and/or so broad that very few circumstances would arise in which a health care professional would be constrained from accessing whatever patient data they wanted to.

An example of such an approach is to be found in the Victorian legislation. Building on the highly permissive wording in the Use and Disclosure Principle enunciated by the Commonwealth Privacy Commissioner, the Victorian Health Privacy Principle 2 expresses a wide array of authorisations, and this appears to have been carried through into the corresponding N.S.W. legislation.

8.3 Statutory Presumption of Consent, With Denials Permitted

This model also assumes that quality of care and convenience to health care professionals dominate the interest in privacy and self-determination, by defining all data as open unless an express denial has been recorded.

Such a scheme would operate as an 'opt-out' arrangement. Any health care professional could access any data, unless the patient concerned had recorded a valid denial of consent that was applicable to that professional in the current situation. Some circumstances might exist in which denials were precluded, or could be over-ridden.

Denials would be applicable to some combination of event, encounter, episode, condition, procedure or medication, together with a list of professionals by identity, category and/or location. The list could be inclusive (i.e. the following are denied access), or exclusive (i.e. all are denied access, except the following). The instance of complete denial would be valid (subject to any statutorily authorised preclusions such as notifiable diseases, and any statutorily authorised over-rides such as court orders).

8.4 Health Care Professional Assertion of Consent, Subject to Controls

Another approach that could be considered is for health care professionals to be required, as a condition of accessing patient data, to make an assertion that consent exists. This could be on the basis of an express consent that they know exists, or an implied consent that they consider exists, or inferred consent, or presumed consent, together with the absence of a denial that affects that health care professional in those particular circumstances.

For this to be a reasonable proxy for a proper consent-based model, a set of controls would need to exist. Each access would need to be logged, together with the assertion that consent exists. The logs would need to be subject to automated and manual analyses in order to detect abnormal patterns. Resources would need to be available to ensure investigation of abnormal patterns. Laws could need to be in place specifying meaningful sanctions for inappropriate access, prosecutions would need to be conducted and sanctions applied, and discovery by aggrieved patients would need to be facilitated in order that civil suits could be pursued.

8.5 Consent-Based Model, With Statutory Authorisations

This model requires that patients be provided with the opportunity to consider what consents and/or denials they wish to provide in relation to their data, and to record them.

Each primary carer would have a form available in several alternative formats such as a printed document, a web-form and a printable electronic file. This would enable patients to declare one of the following;

- **an unqualified, general consent** (although personal data would continue to be subject to the protections that the law provides for health care data);
- **an unqualified, general denial of consent** (which would be subject to such constraints as the law places on that right);
- **a general consent, subject to a specific denial**. The consent and the denial would relate to specific data, which may define:
  - a particular party or category of parties;
  - one or more identified health care events, encounters, episodes, conditions, procedures and/or medications; and/or
  - one or more specific purposes;
- **a general denial, subject to a specific consent**. ; The denial and the consent would relate to specific data, which may define:
  - a particular party or category of parties;
  - one or more identified health care events, encounters, episodes, conditions, procedures and/or medications; and/or
  - one or more specific purposes;
- **a nested sequence of a consent, followed by a more specific denial, followed by a yet more specific consent, etc.**. Each would relate to specific data, as above;
- **a nested sequence of a denial, followed by a more specific consent, followed by a yet more specific denial, etc.**. Each would relate to specific data, as above.

Articulation of such a facility would require analysis, consultation, design, construction, d testing, education and training, and infrastructure. It would demand time and effort from primary carers, and this would need to be reflected in recompense mechanisms. On the other hand, it would significantly improve patient confidence in relation to use and disclosure practices relating to their data.

8.6 Prohibition on Access Without Consent

This is equivalent to a 'gatekeeper' mechanism or access control, as described in section 7.3 above. Such a fully consent-based model involves high weighting on patient privacy and self-determination, to the extent that quality of care, and convenience and practicality for health care professionals, is compromised.

There are circumstances in which this model may be appropriate. For example, a person who is at serious risk of being subject to violence may much prefer to deny access to their data, and compromise their quality of care, in order to deny health care professionals, and hence others, from accidentally or intentionally communicating their data to the people who threaten them.

9. CONCLUSIONS

This document has provided background information relating to consent in health care contexts. Its purpose has been to provide a basis on which e-consent models can be developed in coordinated care.

The analysis culminated in a framework for consent, presented in chapter 7, and a set of possible models for e-consent, presented in chapter 8.

A variety of e-consent models is possible. A set has been outlined, varying from highly permissive to highly constrictive. If e-consent is to be meaningful, in order to encourage patients to have confidence in the manner in which data about them is used and disclosed, the most permissive of the models need to be avoided, and a practical balance found.

REFERENCES

Data Privacy

APC (1994), Australian Privacy Charter', Australian Privacy Charter Council, at http://www.apcc.org.au/Charter.html

AS4400 (1995) 'Personal privacy protection in health care information systems' Standards Australia, 1995

Clarke R. (1997) 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms', at http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html

Health Records (Privacy and Access) Act 1997 (A.C.T.), at http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/index.html

NHMRC (1993) 'Guidelines for the protection of privacy in the conduct of medical research' National Health & Medical Research Council, 1993

NSW Health (1996) 'Information Privacy Code of Practice' Privacy of Information Committee, NSW Health, May 1996, ISBN 0 7310 0773 5, HP No. (IDU) 96-25, Circular No. CPR 96/34

Privacy Act 1988 (Cth), at http://www.austlii.edu.au/au/legis/cth/num%5fact/pa1988108/index.html

Privacy And Personal Information Protection Act 1998 (N.S.W.), at http://www.austlii.edu.au/au/legis/nsw/consol%5fact/papipa1998464/index.html

Privacy of the Person

AAP (1995) 'Informed Consent, Parental Permission, and Assent in Pediatric Practice' Pediatrics 95, 2 (February 1995), at http://www.cirp.org/library/ethics/AAP/

Circumcision Information Resource: Readings in Medical Ethics, at http://www.cirp.org/library/ethics/

HHS (2001) 'General requirements for informed consent' [U.S.] Department Of Health And Human Services, National Institutes Of Health, Office For Protection From Research Risks, para. 46.116-117, at http://ohrp.osophs.dhhs.gov/humansubjects/guidance/45cfr46.htm#46.116

Human Tissue Act 1983 (N.S.W.), , at http://www.austlii.edu.au/au/legis/nsw/consol_act/hta1983160/index.html

NDSU (1994) 'Decisions for Health in North Dakota: Advance Directives and Informed Health Care Consent', HE-494 (Revised), July 1994, at http://ndsuext.nodak.edu/extpubs/yf/fammgmt/he494w.htm

Transplantation And Anatomy Act 1978, (A.C.T.), at http://www.austlii.edu.au/au/legis/act/consol_act/taaa1978298/index.html

APP. 1A: Commonwealth Privacy and Consent Laws

The key legislation is the Privacy Act 1988, as amended, and in particular as amended by the Privacy Amendment (Private Sector) Act 2000, which came into force on 21 December 2001. The complete (and now very complex)Act is at:
Privacy Act 1988, at http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

In general, this applies to health care as it does to every other sector.

In the 'Information Privacy Principles' that regulate the **public sector** (since 1988):

A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the individual concerned has consented to use of the information for that other purpose;

(Principle 10 Limits on use of personal information, at
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.10.html)

Very similar provisions exist in Principle 11 Limits on disclosure of personal information, at:
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s14.11.html

In the 'National Information Privacy Principles' that regulate the **private sector** (since 21 December 2001):

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

…

(b) the individual has consented to the use or disclosure

… [or authority of law, emergency, etc.]

Various qualifications exist in the substantial list of exceptions that follow, some specifically relating to health care contexts. Interpretation is far from straightforward.

10.1 An organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; [or authority of law, emergency, etc.]

Various qualifications exist, some specifically relating to health care contexts.

(Principles 2 Use and Disclosure and 10 Sensitive Information, at
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/sch3national.html)

In relation to **medical research**, the Privacy Act 1988 authorises the National Health and Medical Research Council to issue "guidelines for the protection of privacy in the conduct of medical research".

See s.95 at:
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s95.html
and s.95A at:
http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s95a.html

The s.95 Guidelines are available from:
http://www.nhmrc.gov.au/publications/synopses/e26syn.htm (March 2000)

The s.95A Guidelines are available from:
http://www.nhmrc.gov.au/publications/synopses/e43syn.htm (December 2001)

The scope of each, and the intended difference between them, is far from clear.

The term 'consent' appears frequently in the two sets of Guidelines.

APP. 1B: N.S.W. Health Privacy and Consent Laws

This Appendix provides background to law and policy in New South Wales that relates to consent in the health care sector.

The **Privacy And Personal Information Protection Act 1998**, applies to all public sector agencies. See
http://www.austlii.edu.au/au/legis/nsw/consol%5fact/papipa1998464/index.html

17 Limits on use of personal information
A public sector agency that holds personal information must not use the information for a purpose other than that for which it was collected unless:

(a) the individual to whom the information relates has consented to the use of the information for that other purpose, or ... [authority of law, and emergency]

See http://www.austlii.edu.au/au/legis/nsw/consol%5fact/papipa1998464/s17.html

S,28 (2) A public sector agency is not required to comply with section 19 [re sensitive data, including health-related data] if, in the case of health related information and in circumstances where the consent of the individual to whom the information relates cannot reasonably be obtained, the disclosure is made by an authorised person to another authorised person involved in the care or treatment of the individual. An authorised person is a medical practitioner, health worker, or other official or employee providing health or community services, who is employed or engaged by a public sector agency.

See http://www.austlii.edu.au/au/legis/nsw/consol%5fact/papipa1998464/s19.html and
http://www.austlii.edu.au/au/legis/nsw/consol%5fact/papipa1998464/s28.html

A variety of other N.S.W. statutes contain various provisions that directly affect privacy of patient data. These include:

- the N.S.W. Health Administration Act 1982, at http://www.austlii.edu.au/au/legis/nsw/consol_act/haa1982221/, in particular s.22, at http://www.austlii.edu.au/au/legis/nsw/consol_act/haa1982221/s22.html, and Regulations;
- the Mental Health Act 1990 s.289, at http://www.austlii.edu.au/au/legis/nsw/consol_act/mha1990128/s289.html;
- the Public Health Act 1991 s.75, at http://www.austlii.edu.au/au/legis/nsw/consol_act/pha1991126/s75.html, and s.17 (re HIV), at http://www.austlii.edu.au/au/legis/nsw/consol_act/pha1991126/s17.html;
- Health Professional Registration legislation; and
- the N.S.W. Health Information Privacy Code of Practice, which is a set of guidelines which may well have the force of law under some circumstances (such as cases in negligence).

The **N.S.W. Health Information Privacy Code of Practice**, at http://www.health.nsw.gov.au/iasd/information-privacy/ipcop98/, states that "personal information may not be disclosed without the consent of the subject, except in the specific circumstances set out in this Code" (section 6.1, p.18; section 7.3, p.29).

The N.S.W. Code further states that "other than under [specified] circumstances ..., health care providers have no greater right of access to health records than any other third party ..." (section 7.4.3, p.32).

Of particular interest in relation to **sensitive personal data** is the Public Health Act 1991 s.17, at http://www.austlii.edu.au/au/legis/nsw/consol_act/pha1991126/s17.html. This makes special provisions relating to the identity and the data of a person being tested for, or diagnosed with, a Category 5 medical condition. (This appears to be HIV/AIDS, but the authority relating to Category 5 is not readily apparent).

A new statute was passed and assented to in September 2002. This is the **Health Records and Information Privacy Act 2002**, at:
http://www.parliament.nsw.gov.au/prod/parlment/NSWBills.nsf/1484fd8a7ada6a26ca25691c001793ed/d2d200f8a7ee9da0ca256bce001ca83a/$FILE/b01-059-p04.pdf

Schedule 1 contains a set of Health Privacy Principles. These include reference to consent as the primary basis for use and disclosure of data. The Act does not define consent.

The N.S.W. Act of 2002 would appear to have a close relationship to the Victorian Health Records Act of 2001.

APP. 1C: A.C.T. Health Privacy and Consent Laws

This Appendix provides background to law in the Australian Capital Territory that relates to consent in the health care sector.

The primary legislation in the A.C.T. is the **Health Records (Privacy and Access) Act** 1997, at http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/index.html.

The A.C.T.'s statutory principles to which consent is relevant are expressed in s.5 at:
http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/s5.html
and include:

- Principle 6: Access to health records;
- Principle 9: Limits on use of personal health information; and
- Principle 10: Limits on disclosure of personal health information.

The primary section regulating consent is s.7, at:
http://www.austlii.edu.au/au/legis/act/consol_act/hraaa1997291/s7.html

The A.C.T. Act authorises disclosure without consent for some non-health uses and disclosures, as follows: "If a person reasonably requires access, for the purpose of the management, funding or quality of a health service received, or being received, by a consumer, to personal health information relating to the consumer, the person may have such access, without the consent of the consumer, to the extent reasonably necessary for that purpose", at:
http://www.austlii.edu.au/au/legis/act/consol%5fact/hraaa1997291/s5.html.

APP. 1D: Victorian Health Privacy and Consent Laws

1. Introduction

This Appendix provides background to, and analysis of, law and policy in Victoria that relates to consent in the health care sector.

It comprises four parts:

- a brief examination of laws passed prior to 2000; and
- an outline of the recent privacy legislation;
- an outline of the recent health records legislation;
- mention of a Discussion Paper on information management in Primary Care Partnerships.

2. Laws Passed Prior to 2000

An AustLII search of Victorian 'All Legislation' using 'consent AND health' produces 113 hits, some of which are relevant, but many spurious. A great many of the relevant ones are in the Mental Health Act, plus a few in the Health Services Act. Only 3 are in 2000, 8 are in 1999, and 18 in 1998, and of these only the Mental Health Regulations appearing to be recent relevant sources.

A further source used was a list of 'related legislation' in the Victorian Human Services Department's 'Information Privacy Principles' document of June 1998.

- **Health Services Act 1988**

s.141(2) Confidentiality
http://www.austlii.edu.au/au/legis/vic/consol_act/hsa1988161/s141.html
[Generally,] A [health service] must not, except to the extent necessary [in the performance of expressly authorised, permitted or required actions] **give to any other person**, whether directly or indirectly, **any information** acquired by reason of being [a health service] **if a person** who is or has been a patient in, or has received health services from, a relevant health service **could be identified from that information**. ...

This does not apply to the giving of information with the prior consent of the person to whom it relates or, **if that person has died, with the consent of the senior available next of kin** of that person, but is subject to a very lengthy list of exceptions.

s. 120(1). Powers of inspection
http://www.austlii.edu.au/au/legis/vic/consol_actt/hsa1988161/s120.html
A **visitor** when visiting a designated public hospital or supported residential service in the region may (d) inspect any records required to be kept on the premises by or under this Act. This does not authorise a visitor to inspect a resident's medical records unless the resident consents; or personnel records unless the member of staff consents.

s.126. Secrecy provision
http://www.austlii.edu.au/au/legis/vic/consol_act/hsa1988161/s126.html
A person who is or has at any time been a visitor must not, except to the extent necessary to perform any official duties or to perform or exercise any function or power under this Act, either directly or indirectly, make a record of, or divulge or communicate to any person, any information that is or was acquired by the person by reason of being or having been a visitor or make use of any such information, for any purpose other than the performance of official duties or the performance or exercise of that function or power.

This does not preclude a person from [among other things] producing a document or divulging or communicating information with the prior consent of the person to whom it relates or, **if that person has died, with the consent of the senior available next of kin** of that person.

s.18E. Confidentiality requirements
http://www.austlii.edu.au/au/legis/vic/consol_act/hsa1988161/s18e.html
As for s.126, but applying to a **case mix auditor**

- **Mental Health Act 1986**

s.53B
http://www.austlii.edu.au/au/legis/vic/consol_act/mha1986128/s53b.html
This section defines the requirements for obtaining informed consent in relation to psychosurgery ('care and treatment of people with a mental disorder').

s.57
http://www.austlii.edu.au/au/legis/vic/consol_act/mha1986128/s57.html
This requires informed consent for psycho-surgery. It is subject to the Psychosurgery Review Board.

s.73
http://www.austlii.edu.au/au/legis/vic/consol_act/mha1986128/s73.html
This relates to consent to electro-convulsive therapy.

ss.84, 85
http://www.austlii.edu.au/au/legis/vic/consol_act/mha1986128/s84.html
http://www.austlii.edu.au/au/legis/vic/consol_act/mha1986128/s85.html
In respect of non-psychiatric treatment of a psychiatric patient, these require informed consent or consent of guardian or authorized psychiatrist

s.120A
http://www.austlii.edu.au/au/legis/vic/consol_act/mha1986128/s120a.html
A.120A(3)(a) refers to the "consent of the person ... or, if that person has died, with the consent of the senior available next to kin of that person".

- **Health Act 1958**

s.137
http://www.austlii.edu.au/au/legis/vic/consol_act/ha195869/s137.html

This provides immunity for giving information to the Secretary about an infectious disease, even if given without the consent of the person to whom it relates or the person for whom it was prepared.

- **Cancer Act 1958**

s.60
http://www.austlii.edu.au/au/legis/vic/consol_act/ca195859/s60.html
This provides immunity for giving information to the Secretary about cancer, even if given without the consent of the person to whom it relates or the person for whom it was prepared.

- **The Children And Young Persons Act 1989**

s.271
http://www.austlii.edu.au/au/legis/vic/consol_act/caypa1989278/s271.html
This authorises the Director-General to consent to treatment of children in care, even if that over-rides the consent of the parents.

- **Guardianship And Administration Act 1986**

s.37
http://www.austlii.edu.au/au/legis/vic/consol_act/gaaa1986304/s37.html
A major medical procedure cannot be performed on a represented person unless the consent of the guardian and the Tribunal has been obtained.

3. The Information Privacy Act 2000

This regulates the public sector. The index is at:
http://www.austlii.edu.au/au/legis/vic/consol_act/ipa2000231/index.html

There is no definition of consent in the Act.

The Information Privacy Principles contain similar provisions to the Commonwealth Privacy Act, although the exceptions are differently framed. See 2.1 at:
http://www.austlii.edu.au/au/legis/vic/consol%5fact/ipa2000231/xx3.html

See also 7.2, 7.3, 9.1, 10.1 and 10.2

s.64 expressly addresses the question of a person's capacity to consent or make a request or exercise right of access, and regulates the use of 'authorised representatives'. See:
http://www.austlii.edu.au/au/legis/vic/consol_act/ipa2000231/s64.html

Schedule 2 to the Act defines the terms 'health information' and 'health service'. see:
http://www.austlii.edu.au/au/legis/vic/consol%5fact/ipa2000231/sch2.html

4. The Health Records Act 2001

The Victorian Department of Human Services (which incorporates Health) published a set of **Information Privacy Principles** in June 1998. A revised set was published in

February 1999. **Consent was defined as "the voluntary agreement of the individual or the individual's authorised representative about a proposed action"**.

Further relevant comments were that "[Consent] can be either express or implied. Express consent is provided explicitly, either orally or in writing. It is unequivocal and does not require any inference on the part of the organisation seeking consent. Implied consent arises where consent may be reasonably inferred from the action or inaction of the individual.

"Consent must be meaningful, that is, an individual must understand what has been consented to and the implications of this.

"Consent must also be obtained without coercion".

The Health Records Act 2001 came into force on 1 July 2002. It applies to health, disability, and aged care information handled by a wide range of public and private sector organizations including hospitals, local governments, state government agencies, universities, and the police. See:
http://www.dms.dpc.vic.gov.au/l2d/H/ACT01966/0_3.html

There is no definition of consent in the Act. There are references in the following sections:

- s.28, re information given in confidence;
- s.80 makes it an offence to acquire a consent by means of threat, intimidation or false representation, and to act without consent where consent is required;
- s.85 addresses the question of capacity to consent or make a request or exercise right of access;
- s.95 deals with consents on behalf of deceased persons;
- Principle 1 requires consent in relation to health information **collection** (subject to a vast array of exceptions);
- Principle 2 does the same in respect of **use and disclosure**;
- Principle 7 does similar things in relation to the use of **identifiers**;
- Principle 9 does similar things in relation to **trans-border data flows**.

5. Primary Care Partnerships Information Management

In July 2000, the Department issued a Primary Care Partnerships Information Management Discussion Paper, with submissions requested by 30 September 2000. The concept of 'primary care partnerships' clearly relates very closely to that of 'co-ordinated care'.

The document includes several scenarios involving consent. It identifies as a Critical Success Factor "Privacy—consumers must be fully aware of and voluntarily give their consent to how personal information will be used".

In addition, "A provider may need to seek a suitable carer to give consent if the consumer is incapable of consenting due to factors such as extreme frailty, youth, intellectual disability, mental illness or their state of consciousness".

"The practice of gaining informed consent will vary from agency to agency, and it is regulated by common law (judicial decisions). There is currently no legislation specifically dealing with informed consent".

"Other areas of further work include ... procedures and formats for obtaining client consent".

The paper is available at:
http://www.dhs.vic.gov.au/acmh/ph/pcp/infomgt/index.htm

APP. 2: A Starter Catalogue of Circumstances

This Appendix contains a 'starter list' of circumstances that may involve various forms of patient consent. The intention is to provide an overview of the range of settings involved. This list is complemented by the separately-published list of specific cases that were used to inform the research.

The list makes a working assumption that the term 'health care professional' is inclusive, and encompasses such people as doctors, physiotherapists, psychology professionals, pharmacists, community nurses, social workers, etc. It is independent of the basis of the employment relationship, and encompasses principals, employees, contractors, locums, etc. Occupations that are not 'health care professionals' include non-medical practice managers, nursing aides, secretarial staff, IT staff, transport services providers, cleaners, etc.

The structure used in this Appendix is as follows:

2.1 Personal Data Collection Settings

2.2 Personal Data Disclosure Settings
- Primary Care Settings
  - Disclosures by Health Care Professionals
  - Disclosures by Other Staff
- Hospital Settings
- Third Party Settings

2.3 Settings Involving Proxies for the Patient

2.4 Settings Involving Special Sensitivities

2.1 Personal Data Collection Settings

From the Patient:
- Interviews
- Forms

From Clinical Work:
- Notes
- Discharge Summaries
- Referral Letters

From Other Organisations:
- Other Health Care Professionals
- Health Care Services (e.g. Pathology)
- Hospitals

Emergency Access to Personal Data (e.g. Wallet/Purse)

From Telephone Calls:
- Notes
- Calling Number Identification (CNI)
- Telephone Conversation Recording

2.2 Personal Data Disclosure Settings

2.2.1 Primary Care Settings

(1) Disclosures by Health Care Professionals

Health Care Operational Disclosures:
- Referral Letters
- Requests for Services (e.g. Pathology)
- Discussions with Peers
- Prescriptions
- Team-Members

Notifications:
- Family and Household Health Risk Notifications (incl. Child Abuse)
- Public Health Risk Notifications under Statutory Authority
- Public Health Risk Notifications under Professional Judgement

Requests by Persons Closely Associated with the Person Concerned:
- Guardians
- Partners
- Immediate Family
- Household-Members
- Adoptees

Training of:
- Health Care Professionals
- Training of Health Care Students
- Training of Administrative Staff

Requests by Researchers:
- Public-Funded Researchers
- Academics
- Private Sector Researchers
- Official Registries, e.g. of Communicable Diseases, Cancer

Requests by Complaints-Handling Bodies / Ombudsmen:

- Health Care Complaints Bodies
- Privacy Commissioners
- Ombudsmen
- Professional Registration Boards
- Insurance Complaints Bodies
- Professional Bodies
- Industry Associations
- MPs

Requests by Claims Processors:

- Medicare
- Pharmaceutical Benefits Schemes
- Insurance Companies
- Investigators

Requests by Law Enforcement Agencies (LEAs)

Requests by Courts (including Coroners, Magistrates, Tribunals)

Requests by Lawyers:

- In Relation to Complaints or Suits Against the Person Concerned
- In Relation to Complaints or Suits Against the Data-Holder
- In Relation to Complaints or Suits Against Other Parties
- In Relation to Probate

Requests under FoI Legislation, and under Privacy Legislation

Requests by Government Agencies:

- Benefits Payment Agencies (e.g. Centrelink, DSS, DVA)
- Community Services Agencies
- Immigration
- Foreign Affairs
- Prisons/Corrective Services Agencies
- Registries of Births and Deaths
- Audit Offices
- Guardianship Boards

Requests by Other Organisations:

- Corporations, e.g. in Relation to Selling
- Not-For-Profit Groups, e.g. in Relation to Fundraising
- The Media

(2) Disclosures by Other Staff

Generally, a significant sub-set of those for 1.2.1(a)

2.2.2 Hospital Settings

Generally, a large sub-set of those for 1.2.1(a), plus additional ones, below:

Discharge Summaries

2.2.3 Third-Party Settings

Medicare

Pharmaceutical Benefits Scheme

Insurance company

2.3 Settings Involving Proxies for the Patient

Persons in Loco Parentis

Guardians

Next-of-Kin

Executors

2.4 Settings Involving Special Sensitivities

STD Generally

HIV/AIDS in Particular

Gynaecological Conditions

Persons-At-Risk (e.g. Protected Witnesses, Battered Wives, Undercover Operatives)

Celebrities and VIPs

Identified Data that is presumed by the Patient to be Anonymous