Association for Information Systems
AIS Electronic Library (AISeL)

July 2008

ECONSENT: PROVENANCE, USE AND FUTURE ROLE

sophie cockcroft

UQBS, sophie@business.uq.edu.au

Follow this and additional works at: http://aisel.aisnet.org/pacis2008

ECONSENT: PROVENANCE, USE AND FUTURE ROLE

Cockcroft, Sophie, University of Queensland Business School, University of Queensland, BRISBANE 4072, Australia, sophie@business.uq.edu.au

Abstract

The use of information technology to manage patient consent is an important emerging area of research in health data management. This paper identifies literature, technological advances and current thinking on electronic consent (eConsent). Key issues for health care providers (HCP) and consumers are distilled through a content analysis of a cross section of news reports for the year June 2005 to May 2006. For the study we selected countries that are in the process of adopting shared electronic health records, and took the approach of using media analysis. The press is a professional critic as defined by Sauer and Wilcox (2007).

The topic of electronic consent (eConsent) is closely aligned with issues of information privacy and related legislation, patient rights, and national culture. Clearly, technology is central to the implementation of eConsent and there are pressing management and security issues to be addressed. This paper will make clear the relationships between these fields of study and comment on the 'state of play' in integrated electronic health record systems today, outlining potential pitfalls.

Keywords: eConsent, Electronic Health Records, Media Analysis.

1   INTRODUCTION

In the past decade the collection, storage and use of individual health and medical data has become increasingly computerized, with the result that it can be collated, stored, analyzed and distributed in unprecedented quantities and put to diverse uses (Manning, 1995). Health insurers, for example, can not only tap patient data for claims payment, they use it for utilization review, underwriting and coverage decisions. Employers use health data to reduce their health care and workers compensation costs, as well as to identify employees who may be costly in the future. Health care providers use the data for research, to collect reimbursement, coordinate diagnosis and treatment and conduct quality assurance. Clinical data repositories and management systems will likely reduce health care costs and improve patient care.

It is in this climate that industrialized nations are seeking to develop centralized online health records for their citizens. Many benefits of this approach are foreseen, but the health record, conventional information systems are extraordinarily hard to manage. (Beale, 2005) put this well in his recent synopsis, stating that, banking and airline systems' customers or travellers are "grossly simplified abstract versions of a person" by contrast, patients in a clinical system have a biological and social complexity far beyond that demanded of other systems. Added to this there are quite considerable challenges and paradoxes inherent in health systems such as mobility of patients, multiple HCPs, and constant changes in technology and the law. The work presented in this study explores the paradox of privacy versus the "need to know". The electronic health record needs to be consent based, with potentially fine grained privacy rules on information use, with exceptions for emergency access. EConsent is at the confluence of Healthcare, Information Technology and Law as illustrated in Figure 1.
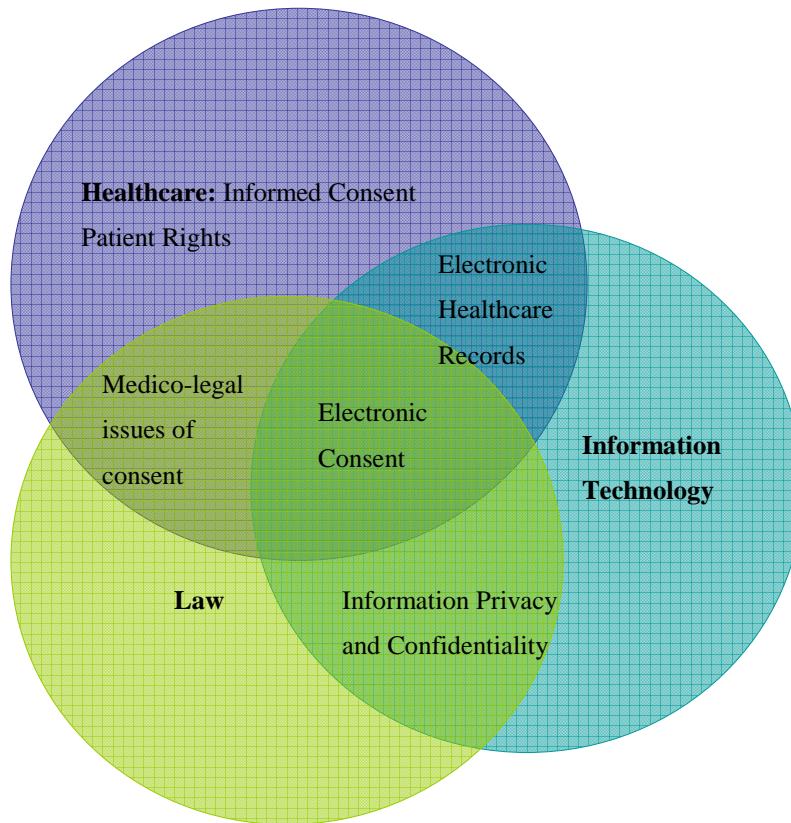
Figure 1 Influences on Electronic Consent

This paper draws together academic literature from the three disciplines to put forward a framework of issues in developing shared electronic health record systems generally, and eConsent systems in particular. Using this framework a content analysis of major news and business publications is performed. This approach is common in the Communications literature (Andsager and Powers, 2001), and whilst it is not common in Information Systems research, it provides evidence to support other literature in the area, and an originality of this study. The news media are charged with covering issues in a balanced and informative manner. These issues are framed for the public by newspapers using particular language and opinions, which in turn feedback the weight of public opinion to policy makers. The aim of this work is to explore the media's role in public perception of electronic consent. The results of this analysis provide a snapshot of the main concerns held by the public and thus the hurdles facing governments and the bodies they entrust with implementing their visions of integrated healthcare. The paper proceeds as follows; eConsent is placed in the context of patient consent, legislative frameworks and Information Technology. Global solutions to electronic health records are described, focusing on how interoperability and access control are achieved. The benefits and pitfalls of EHRs are presented, focusing on eConsent and leading to a framework of issues which act as a lens for reviewing media coverage of the same.

2   THE HEALTHCARE PERSPECTIVE

Before discussing electronic consent, the underlying health data issue of informed consent needs to be addressed.

'Informed consent' and 'patient consent' are used in health care environments to describe an agreement that occurs between healthcare provider and consumer. The term 'patient consent' means that a person receiving health care is willing to share personal health information and where appropriate to receive a course of medical treatment. Informed consent has a very particular meaning, and has been the subject of some controversy. Informed consent requires that the patient is informed, before any request for information, or treatment, of the following: Who will access their record, how it will be shared, what the information will be used for, and the risks associated with the prescribed medical treatment or clinical trial (Galpottage & Norris, 2004).

Informed consent derives from three important principles of bioethics; non-malfeasance (prohibition of doing harm) beneficence (the act of doing good) and autonomy (the right of choice). In the context of informed consent, if a health care provider were to knowingly omit to tell a patient the consequences of their consent or the use to be made of their information it would be an act of malfeasance. By contrast, beneficence would be demonstrated in a situation where the health care provider took due care to ensure the patient was as informed as possible about all consequences. Lastly, autonomy dictates that the patient, being informed, should be allowed to make their own choices without undue influence or persuasion.

3   LEGAL PERSPECTIVE

It is interesting to note that many countries do not have a codified law of informed consent, but rely on best practice and guidelines put forward in patient's charters. However, whether encoded or not, the law or patients charters/ HCP guidelines cover the same areas. Broadly, these relate to the right to information, the right to informed consent (including the right not to be informed) the right to withdraw from treatment, the right to autonomy and dignity, the right to have a representative, the right to choose your provider and the right to privacy and confidentiality. Additionally, patients find themselves in situations of express consent where the fact that the patient signs a document, provides legal evidence that permission for the treatment or data use was given. Alternatively in
Implied consent, the patient is assumed to have been given consent by, for example, raising their sleeve to have blood taken. Finally there are various exclusions to the need to obtain consent. These are; the case of a legal proxy, where someone gives consent on the patient's behalf, where a patient has given consent by prior arrangement, or in an emergency, or under certain mental health or public health conditions. For the purposes of this study we concentrate on the personal information aspects of informed consent. In terms of patients rights (not restricted to any jurisdiction) these information aspects impact upon; the right to access medical files/medical records, the right to privacy and confidentiality (disclosure only with consent) and exception for emergency cases (unless prior refusal given e.g. refusal for blood transfusion). In addition to laws/charters specifically relating to health, there are well established data protection laws which are described elsewhere - see for example Privacy International (2002).

4   THE IMPACTS OF TECHNOLOGY ON CONSENT

Management of consent to access medical records has been impacted by developments in electronic health records. An electronic health record is supposed to be a repository of information regarding a person's health status in computerized form which can be stored and transmitted securely. According to ISO/TC215 WG1 its "primary purpose is the support of continuing efficient and quality integrated

health care and it contains information that is retrospective, concurrent and prospective". This level of computerization provides an opportunity for both HCPs and patients to clearly identify their needs and preferences with respect to privacy and access to their own health records.

Much work has been done to put consent into action in information systems through the concept of eConsent. There are increasingly well developed models of the eConsent data structure or eCo (Coiera & Clarke, 2004; O'Keefe, Greenfield, & Goodchild, 2005; O'Keefe et al., 2002). Three issues emerge from the development of these models; information sharing, granularity of the consent concept, and support for consent as a dynamic changing process.

The trust relationship between provider and consumer in most eCo prototypes is assumed to assist information sharing. In order to provide comprehensive health care, much patient data must be shared between nurses, and physicians in both primary and secondary care, and test results need to flow freely between these and other HCPs.

In the eCo literature, consent is modelled to a finer granularity than legislative models have yet achieved, for example, whilst a patient has a right to choose their provider it is not a right to decide which provider sees which part of your record and for what purpose, this is clearly due to the need for legal concepts to be tested and made law, if indeed it is possible to legislate at this level.

Four different levels of "opt-in" are modelled: General denial, general denial and inclusions, general consent and exclusions, and general consent. These have profound effects on the balance between clinical access and patient privacy. The relationship between information and consent is illustrated as a full set of dimensions below.

Access to <information>
By an <entity>
for a <purpose>
in a <context>
is {consented to| denied}

However eCos are restricted, by necessity, to express consent.

5   IMPLEMENTATION

An eCo exists as a data structure attached to a health record, which could be converted to XML and transmitted with the record if necessary. The system that manages the eCo could operate in a number of ways for example it could be through a "gatekeeper systems" which blocks unauthorized individuals from accessing information, an "audit system" which allows unrestricted access, but obtrusively records all accesses where the individual must be prepared to assert that their access is justified or a "Passive Record". The passive record would fulfil all legal requirements described here, by simply recording in a text file the nature of consent agreements, but they are ineffective in a distributed environment. In a distributed system the eCo follows the EHR around and the currency of its linkage to the record has to be managed.

Reflecting that consent is not a static process, an eCo is programmed to expire after a given time.

Another initiative pioneered in the US by NEC (2006) is the use of tablet PCs, with electronic consent forms, to gather and store electronically, consent information from patients. The system developed by NEC is called PersonalPass and is designed to make administration of consent and HIPAA forms

easier. In terms of the classification laid out above, such systems are a passive record, in that they are really no different than a digitized form, except that they have certain integrity constraints on entry which assure the quality of the data entered. The relevance of this work to the current work is that this type of electronic consent supports consent for clinical intervention in particular, whereas the eCo structure is designed primarily to support consent to access data.

5.1   Global solutions to informed consent and health information access control – Canada, NZ, Australia, UK and USA

5.1.1   Sharable lifelong health records

The lifelong shareable health record is becoming an accepted concept the world over. Many countries are investing large amounts of money in national systems to with the aim of improving health care. As part of the United Kingdom's National Programme for Information Technology (NPfIT) initiative (Currie & Guah, 2006) a database is being installed which will allow healthcare providers to access a patient's records wherever they are. The aim is to connect every family doctor and hospital in England, and provide online records for 50 million patients by 2010.

In Canada a shareable centralized health record is being developed by Canada health Infoway (2006). The blueprint for and electronic health record solution produced by Infoway is highly regarded, and has positioned Canada as a world leader in Electronic Health Record Management (Hovenga, Garde, & Heard, 2005)

In Australia an initiative with the same aim "HealthConnect" (2006) is underway. Health connect is slated to come with smart card technology whereby secure access to health connect can be provided. The Health connect system combines a plethora of medical record databases (community/diagnostic/general practice and tertiary levels) into one central network (Grain, 2003).

Almost all general practices in New Zealand and computerized and most practices (93.7%) connect to a system called HealthLink, so they have the capability of transferring data electronically (Didham, Martin, Wood, & Harrison, 2004). They use HealthLink's secure system to electronically exchange sensitive patient data such as test results, discharge summaries and referrals. New Zealand benefits from two decades of a patient master index, rather than a unique Health ID number, which allows records to be more readily shared between providers. It already has a nationwide health data network and an adverse medical reaction system. Web portal technologies are installed in 60% of New Zealand hospitals

In the US, the department of health and human service is planning the design and development of a National Health Information Network (NHIN) to facilitate exchange of health care information nationwide while protecting patient privacy. In early 2005 500 proposals for the NHIN were received. Four teams were picked to prototype the NHIN in late 2005, it is planned that these systems are in production by the end of 2006 (Kaushal, Bates, Poon, Jha, & al, 2005).

5.1.2   Information Access Control

The confidentiality of personal information shared with a clinician in the context of treatment is a fundamental obligation in the provision of health care services. The clinician must also have consent of the patient to share that information with a third party. As health care providers adopt integrated systems based on internet technology for information exchange, it becomes increasingly difficult to honour this obligation. As personal health information is exchanged with an increasing number of stakeholders, there is a risk that information being accessed in ways for which the patient had not given consent. Practices such as emailing health information are quite common, but clinicians are

becoming increasingly uncomfortable with this, many expressing the need for health information to go straight into their databases (O'Keefe, Greenfield, & Goodchild, 2005)

In setting up such systems developers need to contemplate how much centralization is acceptable to stakeholders. In a fully centralized system such as NPfIT consent management is simplified, but there are perceived privacy risks and performance issues, leaving it decentralized leaves consent management to the consumer. However, to mitigate this responsibility, default policies can be set up. With a decentralized system, such as the system described in O'Keefe et al. (2002, 2005) as health records are transferred between facilities the eConsent record becomes part of the health record. Clearly this establishes an imperative to manage this additional health data and its currency at all sites where it is downloaded. This is done by means of a "placeholder" which identifies which parts of the record can be seen by whom and for what purpose, and which travels with the record. The NPfIT solution involves an analogous solution the "sealed envelope" where parts of the record can only be seen in emergencies. The default is for HCPs to see a summary record only which will only contain data on major diagnoses, surgical procedures, allergies and prescriptions, which some have criticized as less than useful (Bostock, 2005). The main healthcare provider can see the whole record.

5.1.3   Benefits of Shared Electronic Health Records

Nations campaigning to adopt national electronic health records recognize potential advantages, to the consumer of health care these include; more rapid and easier access to care, smoother transitions between primary and secondary care, definite appointment slots at convenient times and shorter waits, more control for over who can access their health information and active participation in decisions about their health care. The benefits suggested for providers are; rapid diagnosis and discharge, seamless support in the community after discharge, avoidance of unnecessary testing and more time to devote to direct care. For those who seek to measure and manage outcomes there is the opportunity to reduce medical errors, improve quality of care, improve patient compliance, lower transaction costs for outpatient testing and prescriptions and reduce variability in clinical care. From a public health point of view there shared health records allow for improvement in health through real-time disease surveillance and monitoring, and by extension to bioterrorism, such records can bolster homeland security. For administrators there will be rapid access to vital and accurate health information, greater portability of health records for an increasingly mobile population and reduced duplication of services.

5.1.4   Issues in shared electronic health records

Previous authors (Grain, 2003) have noted the following problems; the issue of how health professionals access to records should be managed, how individuals can limit access to their own records or identify the appropriate circumstances for those records to be accessed, and whether health professionals are aware of the level of access they really have. This issue was foreshadowed earlier in the paper with the description of summary versus full records and the exception for emergencies which is solved differently depending on the level of centralization of the record. At a macro level health record sharing is impacted by different government regulation, different cultures and differing attitudes to information privacy (Sandhu, 2006). Further, the level of opt-in patients should be given by default is frequently questioned in the literature (Edwards, 2005 ; Kaushal, Bates, Poon, Jha, & al, 2005). One reason for this, is that data protection laws can have a severe impact on epidemiological studies (Breen, 2001 ; Magnusson, 2002 ; Vedig & Vedig, 2002). If researchers were required to get explicit consent from patients every time their data was to be used, the whole process would grind to a halt. Recently (Iversen, Liddell, Fear, Hotopf, & Wessely) described this issue in the context of research on the health of military personnel. Frequently, authors comment on how our current understanding about the links between smoking and lung cancer would not have been possible had

data protection laws been as strict in the 1950s and 60s. There is a clear need for standards in health records, to facilitate interoperability(Hovenga, Garde, & Heard, 2005), and these include standards for consent. Finally a peripheral issue is and the cost of implementing such systems (Simons, 2006)

6   METHODOLOGY

The study focuses on a calendar year of stories derived from Factiva (2006) for the period from May 2005 to April 2006. Five OECD countries ensconced in development of national heath data networks were selected for comparison. Initially the following query was used.

(consent or eConsent or ("access control")) and (data or ehr) and ns=GHEA and rst=TMNB

and(re=AUSTR or re=UK or re=CANA or re=USA or re=NZ)

The above search queries stories from the healthcare area in major news and business publications. This resulted in a total of 357 stories. Due to the small number of publications from Canada, NZ and Australia the search was widened to include all publications from these regions this resulted in 426 stories. On analysis a large number of these stories (85) related to specific drug trials and for each country particular issues came to the fore that were irrelevant for the purposes of this study. For example In New Zealand much debate raged on the topic of meningococcal infections, whereas in the UK a story about an eye surgeon who had done a study without first gathering the patients' consent dominated the headlines. Stories relating to costs were excluded these formed a large part of the debate in the US. A total of 268 stories were deemed irrelevant, leaving a usable pool of 73 stories. NZ did not appear in this selection. It appears integration is not a key issue in NZ today. Perhaps surprisingly for a small country New Zealand has an advanced health IT infrastructure. Thus it is excluded from the discussion at this point. We used both traditional content analysis and a computer assisted content analysis program, Termine (2008).Two coders looked at each story and identified the main areas of coverage by source and by country and classified based on issues identified from the academic literature; Smartcard security, Opt in, Confidentiality, Research, Standards, the use of a "sealed envelope" for emergency access, and access control. The articles were read thoroughly to examine evidence for the use of themes identified and to search for new themes or frames that may have been overlooked. The results of this initial analysis are illustrated in Table 1.

Country	Issue								
	Smartcard Security	Opt-In	Confidentiality	Research	Gene	Envelope	RMC*	Systems	Total
Australia	1	2	5	1	1			4	14
Canada				5					5
UK	4	3	6	11	1	4	3	6	38
USA		14	1	1					16
	5	19	12	18	2	4	3	10	73

Table 1 Breakdown of News Stories

In addition to these elements in Table 1 the column labelled RMC* refers to a particular issue evolving in the UK as demand for care outstrips supply, strategies to manage demand have evolved involving. telephone help lines, computer based decision support systems, and practitioner-led triage systems which together comprise the RMC concern has arisen that thousands of GPs who refer via these centres risk legal action or being struck off if they fail to warn patients that data will be seen by a third party.

7 RESULTS

A great deal of concern arose from smartcard security, particularly following a highly publicized trial of the same in Tasmania Australia, related to this issues of confidentiality arose around smartcard access in Australia, and around the summary record in the UK, which is still thought to be too readily accessible by many. The level of opt-in or opt-out provided by default raised some interest as did the related issue of the damaging effects on epidemiological research of stringent privacy and consent laws. The "sealed envelope" and the possibility of overriding consent in an emergency were of interest, and finally some concern was expressed over storage of genetic information in shared database systems. Ten of the stories described the systems in place in the various countries of the study. This prompted a more fine grained analysis using the systems themselves as the search criteria the results of this search are shown in Table 2.

Country	Query	No of Results	Most frequently cited issue
Australia	"healthconnect" and rst=TMNB and re=AUSTR	41	Confidentiality
USA	National Health Information Network and rst=TMNB and re=USA	12	Standards
UK	NPfIT and rst=TMNB and re=UK	23	Confidentiality
Canada	"Canada health infoway" and rst=TMNB and re=cana	3	Interoperability/Standards

Table 2 Summary of stories on e-Health Initiatives

8 DISCUSSION AND CONCLUSION

The UK project NPfIT is often cited as the world's largest civil IT project, it is drawing much publicity and interest around the world. As a result of the decision to centralize the records, much fear of breaches confidentiality and loss of control is being fuelled. The issue of consent here is how much of the patients records should be seen and by whom. A default situation is in place where a summary record can be seen by all, but the full record only by the key health provider patients can opt to have their records put on the data "spine" in the first place or not. In all countries contemplating shareable lifelong health records standards and interoperability are an issue this seems to be more pressing in the US, perhaps due to the diversity of the systems and the physical and political separation of the states. These issues are not directly of concern in eConsent, however eConsent should be of concern when

setting such standards, so that an eCo can readily be attached to any records that emerge. The ability to access records in an emergency is important, this is one of the exceptions to consent outlined in the discussion on legislation.

We live in an interesting time with respect to health records, whilst a shared record holds the promise of better and more efficient health care, it also introduces privacy and security concerns. Adoption of standards by nations is seriously impacted by the prevailing legislation which is in turn affected by culture. Identifying and mitigating these cultural differences is the subject for further work.

9 REFERENCES

Andsager, J. Powers, A. (2001) Framing Women's Health With a Sense-Making Approach: Magazine Coverage of Breast Cancer and Implants Health Communication, Volume 13, Issue 2, 2001, Pages 163 – 185.

Beale, T. (2005). The health record—why is it so hard?. In: R. Haux and C. Kulikowski, Editors, IMIA Yearbook of Medical Informatics 2005: Ubiquitous Health Care Systems, Stuttgart, Schattauer (2005), pp. 301–304.

Bostock, N. (2005). GPs want further detail on shared care records. GP (General Practitioner), 7.

Breen, K. J. (2001). Consent for the linkage of data for public health research: is it (or should it be) an absolute pre-requisite? . Australian and New Zealand Journal of Public Health 25 (5), 423-425

Coiera, E., & Clarke, R. (2004). e-Consent: The design and implementation of consumer consent mechanisms in an electronic environment. Journal of the American Medical Informatics Association, 11(2), 129-140.

Currie, W., & Guah, M. (2006). IT-ENABLED HEALTHCARE DELIVERY: THE U.K. NATIONAL HEALTH SERVICE. Information Systems Management, 23(2), 7-22.

Didham, R., Martin, I., Wood, R., & Harrison, K. (2004). Information Technology systems in general practice medicine in New Zealand. The New Zealand Medical Journal, 117(1198), 1-4.

Edwards, S. (2005). Electronic health records and consent NCOSS News 32 (6), 18-19

Factiva. (2006). Factiva: Dow Jones and Reuters. from www.factiva.com. Accessed 28/4/2008

Galpottage, P. A. B., & Norris, A. C. (2004, June, 2004). Patient Consent Principles and Guidelines for E-Consent: A New Zealand Perspective. Paper presented at the iSHIMR2004, Proceedings of the Ninth International Symposium on Health Information Management Research, Sheffield.

Grain, H. (2003). Health information managers and electronic health records: The impact of e-consent. Health Information Management Journal., 33(3), 84-88.

HealthConnect. (2006). About HealthConnect. Retrieved 01/05/2006, from http://www.healthconnect.gov.au/about/index.htm

Hovenga, E., Garde, S., & Heard, S. (2005). Nursing constraint models for electronic health records: A vision for domain knowledge governance. International Journal of Medical Informatics Nursing Informatics Special Issue, 74(11-12), 886-898.

Infoway. (2006). Canada Health Infoway. Retrieved 28/04/2006, 2006, from http://www.infoway-inforoute.ca/en/home/home.aspx

Iversen, A., Liddell, K., Fear, N., Hotopf, M., & Wessely, S. (2006) Epidemiology: Consent, confidentiality, and the Data Protection Act. British Medical Journal, 332(7534), 165.

Kaushal, R., Bates, D. W., Poon, E. G., Jha, A. K., & al, e. (2005). Functional Gaps In Attaining A National Health Information Network. Health Affairs, 24(5), 1281.

Magnusson, R. S. (2002). Data linkage, health research and privacy: regulating data flows in Australia's health information system. . Sydney Law Review 24 (1), 5-55

Manning, W. (1995). Privacy and confidentiality in clinical data management systems: why you should guard the safe. from www.netreach.net/~wmanning/cdm.htm .

NEC. (2006). Electronic Consent Forms. Retrieved 28/04/2006, 2006, from http://www.necsam.com/HealthCare/PersonalPass/eConsent.cfm

O'Keefe, C. M., Greenfield, P., & Goodchild, A. (2005). A decentralised approach to electronic consent and health information access control. Journal of Research and Practice in Information Technology, 37(2), 161-178.

O'Keefe, C., Goodchild, A., Greenfield, P., Waugh, A., Cheung, E., & Austin, D. (2002). Implementation of Electronic Consent Mechanisms (No. Version 1.0). BRISBANE: DSTC, CSIRO.

Privacy International. (2002, Updated Continuously). Privacy International.   Retrieved 29/01/02, 2002, from http://www.privacyinternational.org/

Sandhu, N. (2006, April 30 - May 3 2006). National Health Information Management/

Information Technology Priorities - An International Comparative Study. Paper presented at the E-Health For Everyone, Victoria, Canada.

Sauer, C., & Willcocks, L. (2007). Unreasonable expectations - NHS IT, Greek choruses and the games institutions play around mega-programmes. J Inf technol, 22(3), 195-201.

Simons, M. (2006). NHS IT NHS system security criticised. Computer Weekly, 4.

Termine (2008) Nactem The National Centre for Text Mining http://www.nactem.ac.uk/software/termine/ accessed 28/04/2008

Vedig, M. D., & Vedig, D. A. (2002). Current privacy law governing the Australian health sector: implications for research and 'audit' Critical Care and Resuscitation 4 (no,3), 231-237