THE ADVANTAGES OF E-HEALTH AND ITS IMPACT ON PATIENT'S RIGHT OF PRIVACY

MUH. ENDRIYO SUSILA
Faculty of Law, Muhammadiyah University of Yogyakarta

ABSTRACT

E-health has become a life style in many countries. The emergence of e-health was an avoidable consequence of the development of the information and communication technology in the world. It is undeniable that e-health offers both quick and comfortable health service. It introduces a new form of relationship between health care provider and health care receiver. However, it also brings bad impact, especially related to the patient's right of privacy. In order to protect the patient's right of privacy from any transgression, a specific regulation governing e-health is needed. Such a regulation has existed in many countries including in Malaysia. In Malaysia, the government has enacted Personal Data Protection Act 2005. The purpose of this paper is to explore the advantages of e-Health on serving the modern society and its negative impacts, especially pertaining to the issue of privacy. The discussion regarding privacy will be focused on the privacy of patient who enters into new form of relationship with healthcare service provider through internet.

Keywords: e-health, telemedicine, privacy

I. INTRODUCTION

The advancement of technology has obviously changed the life style of people in modern society. The presence of the information and communication technology for example, has reduced the frequency of face to face meeting among the partners in many kinds of business transaction, since the internet has taken it over. The internet has enabled a client of a bank to make transaction without attending to the counter of the bank and filling out some forms. It constitutes a kind of new services provided by the bank under the concept of E-Banking.

Nowadays, such a model of transaction has also been adopted into healthcare service, known as what so-called 'telemedicine' or in broader sense 'telehealth'. Telemedicine is developed to provide better care to patients in remote locations, and to allow consultation with specialists without the necessity of costly and difficult travel.

Telemedicine is one of services offered in e-health. Besides enjoying a better healthcare service through telemedicine and telehealth, people can also improve their knowledge on health as well as health products by browsing e-health sites. Millions of consumers worldwide are using the internet to obtain quality health information directly affecting their lives making this form of telemedicine an important new tool for improving healthcare (http://www.atmeda.org/ehealth/guide.htm).

Internet has a significant role in increasing the quality of healthcare. Since health record can be collected electronically, healthcare service becomes more efficient in term of time and cost. However, the development of electronic health records does raise significant issues over the privacy and security of health data. It is not the creation of an electronic record per se that creates privacy concerns — rather it is the capacity for electronic records to be linked electronically (over networks or over the internet) and to be accessed by multiple individuals, or for unauthorized access, that creates privacy concerns (Bennet, 2001, “retrieved from http://www.lexis.com).

Privacy has emerged as a major issue for e-health initiatives. In recent years, consumers have become a lot more wary about the collection and use of their personal information. Modern computing capabilities mean that huge quantities of data can be stored, sorted or accessed by large numbers of people in ways that was not possible in the days of paper-only records (Bennet, 2001, “retrieved from http://www.lexis.com).

E-health has become a life style in many countries. The emergence of e-health was an avoidable consequence of the development of the information and communication technology in the world. It is undeniable that e-health offers both quick and comfortable health service. It introduces a new form of relationship between health care provider and health care receiver. However, it also brings bad impact, especially related to the patient’s right of privacy.

Based on all explanation having mentioned above, the question is how to protect the right of privacy of the patient who involves in e-health.

II. DEFINITION OF E-HEALTH

This term is used to characterize not only “internet medicine”, but also virtually everything related to computers and medicine. The term was apparently first used by industry leaders and marketing people rather than academics. It seems quite clear that e-health encompasses more than a mere technological development (Eysenbach, 2001, “retrieved from http://www.jmir.org/2001/2/e20).

E-health is an emerging field in the intersection of medical informatics, public health and business, referring to health services and information delivered or enhanced through the

Internet and related technologies. In a broader sense, the term characterizes not only a technical development, but also a state-of-mind, a way of thinking, an attitude, and a commitment for networked, global thinking, to improve health care locally, regionally, and worldwide by using information and communication technology (Eysenbach, 2001, "retrieved from http://www.jmir.org/2001/2/e20).

E-Health is a consumer-centred model of health care where stakeholders collaborate, utilizing ICTs, including internet technologies to manage health, arrange, deliver and account for care, and manage the health care system (Alvarez, "retrieved http://www.ehealthinternational.net/popups/articles/window.php*).*

III. THE SCOPE OF E-HEALTH

The term e-Health has been used to describe a variety of activities including almost any electronic exchange of health-related data, voice or video. E-health serves several activities as follows; *(Alvarez,* "retrieved from http://www.ehealthinternational.net/popups/articles/window.php*)*

a. purchase drug prescription
b. consultation
c. access to medical record
d. manage personal health information on the world wide web
e. communication.

From the explanation above, it is clear that e-health constitutes a general term embracing telemedicine, telehealth, and health informatics, which all are developed as important components of the modern health care system.

While each of these components is related to the other, there are important differences between them. *Telemedicine* has been defined as 'a system of health care delivery in which physicians examine distant patients through the use of telecommunications technology.' It is important to realize that while telemedicine is often thought of as a development of the late 20th Century, it has in fact been around for much longer. The telegraph was used to obtain medical advice in the early 20th Century in outback Australia, and in 1928 the first base for the Flying Doctor was established in western Queensland, and a 'significant factor in its early success was the "pedal wireless"'. Developments in technology will also have an impact on perceptions of telemedicine as 'it will be difficult to separate telemedicine from other health related activities that use information and communication technologies (Bennet, 2001, "retrieved from http://www.lexis.com).

In contrast to telemedicine, the term *telehealth* suggests a broader application which takes account of the activities of a range of health professionals, including nurses, psychologists and others. Clearly the use of information technologies is an integral part of the electronic delivery of health care (Bennet, 2001, "retrieved from http://www.lexis.com).

The use of these technologies poses a variety of broader issues about the management and use of information. This is the field of health informatics. The Health Informatics Society of Australia defines *health informatics* as an evolving scientific discipline that deals with the collection, storage, retrieval, communication and optimal use of health related data, information and knowledge. The discipline utilizes the methods and technologies of the information sciences for the purposes of problem solving and decision-making thus assuring quality healthcare in all basic and applied areas of biomedical sciences (Bennet, 2001, "retrieved from http://www.lexis.com).

While telemedicine and telehealth tend to be focused on the delivery of healthcare to remote patients, *e-health* encompasses both the remote delivery of health care and health information as well as the health sector aspects of e-commerce. E-health has been defined as 'the use in the health sector of digital data — transmitted, stored and retrieved electronically -- for clinical, educational and administrative purposes, both at the local site and at a distance.' While the delivery of health care to remote patients is an important and highly visible aspect of the electronic dimensions in modern health care, the integration of broader developments in the information economy into the health sector promises to bring significant change, at the organizational or institutional level, as health-related business-to-business commerce realizes the efficiencies of electronic business transactions (Bennet, 2001, "retrieved from http://www.lexis.com).

IV. THE ADVANTAGES OF E-HEALTH

The internet has the potential to change the way that patients and health professionals interact. It is for example, possible for patients to correspond with their health professionals by email. The widespread availability of the internet means that patients have access to unprecedented amounts of health information. This may be a positive development, with patients more educated about health and health care. However, it may also mean that patients come to doctors and other health professionals with health-related information obtained from the internet, which may or may not be accurate (Bennet, 2001, "retrieved from http://www.lexis.com).

The advantages of e-health sometimes can be described as the 10 E's as follows: (Eysenbach, 2001).

1. Efficiency – one of the promises of e-health is to increase efficiency in health care, thereby decreasing costs. One possible way of decreasing costs would be by avoiding duplicative or unnecessary diagnostic or therapeutic interventions, through enhanced communication possibilities between health care establishments, and through patient involvement.

2. Enhancing quality of care – increasing efficiency involves not only reducing costs, but at the same time improving quality. E-health may enhance the quality of health care for example by allowing comparisons between different providers, involving consumers as additional power for quality assurance, and directing patient streams to the best quality providers.
3. Evidence based – e-health interventions should be evidence-based in a sense that their effectiveness and efficiency should not be assumed but proven by rigorous scientific evaluation. Much work still has to be done in this area.
4. Empowerment of consumers and patients – by making the knowledge bases of medicine and personal electronic records accessible to consumers over the Internet, e-health opens new avenues for patient-centered medicine, and enables evidence-based patient choice.
5. Encouragement of a new relationship between the patient and health professional, towards a true partnership, where decisions are made in a shared manner.
6. Education of physicians through online sources (continuing medical education) and consumers (health education, tailored preventive information for consumers)
7. Enabling information exchange and communication in a standardized way between health care establishments.
8. Extending the scope of health care beyond its conventional boundaries. This is meant in both a geographical sense as well as in a conceptual sense. E-health enables consumers to easily obtain health services online from global providers. These services can range from simple advice to more complex interventions or products such as pharmaceuticals.
9. Ethics – e-health involves new forms of patient-physician interaction and poses new challenges and threats to ethical issues such as online professional practice, informed consent, privacy and equity issues.
10. Equity – to make health care more equitable is one of the promises of e-health, but at the same time there is a considerable threat that e-health may deepen the gap between the "haves" and "have-nots". People, who do not have the money, skills, and access to computers and networks, cannot use computers effectively. As a result, these patient populations (which would actually benefit the most from health information) are those who are the least likely to benefit from advances in information technology, unless political measures ensure equitable access for all. The digital divide currently runs between rural vs. urban populations, rich vs. poor, young vs. old, male vs. female people, and between neglected/rare vs. common diseases.

V. THE IMPACT OF E-HEALTH ON PATIENT'S RIGHT OF PRIVACY

Before entering into discussion regarding the impact of e-health on patient's right of privacy, some basic principles pertaining to privacy and some other related terms will prior to be discussed.

1. THE CONCEPT OF PRIVACY

Privacy is a broad concept which has been defined in many different ways. It may encompass a number of aspects, but generally, refers to the right or capacity to shield some aspects of one's life from the scrutiny of others, to draw a boundary between the public and private spheres of one's existence (Tigerstrom, "retrieved from http://www.lexis.com). Justice Louis Brandeis defines privacy as the right to be left alone — the most comprehensive of rights, and the right most valued by a free people (*Olmstead v. U.S.* (1928)

The particular aspect of privacy which is at issue here is sometimes referred to as "information privacy": the right to control when, how and by whom personal information about oneself is communicated to and used by others. Personal information, in turn, can be defined as any information about an individual which may be identified with that individual in some way. This identification need not be by name or even by anything so obvious as an identification number; there are many ways in which information may be traced to its subject, and technology is increasing the number of ways in which this may be done, by facilitating the matching of data sets, for example. Whenever data may be traced to its subject, it has the potential to reveal private information about that person and is thus considered sensitive (Tigerstrom, "retrieved from http://www.lexis.com).

General speaking, information privacy is the ability of an individual to control the use and dissemination of information that relates to himself or herself. It relates to confidentiality and security. Confidentiality *is a tool for protecting privacy. Sensitive information is accorded a confidential status that mandates specific controls, including strict limitations on access and disclosure. These controls must be adhered to by those handling the information.* Security *is all the safeguards in a computer-based information system. Security protects both the system and the information contained within it from unauthorized access and misuse, and accidental damage* (http://www.ntia.doc.gov/reports/telemedicine/privacy.htm).

2. THE SCOPE OF PRIVACY IN E-HEALTH

'Privacy' is a vaguely defined term that, in an online context, includes the right of an individual to:

· Determine what information is collected about them and how it is used. Sometimes we are not aware what data are being collected about us (e.g. via 'cookies' on a Web site—see Glossary) or how it may be used. Registering with a Web site (i.e. giving your name, email address, medical registration number, etc.), for example, may enable that site to keep track of what you—a readily identifiable individual—view or spend online. Such information could be passed on to third parties. Some sites publish 'privacy policies' in an attempt to inform users and reduce the chances of patients or healthcare professionals placing their privacy at risk.

- Access information held about them and know that it is accurate and safe.
- Anonymity (e.g. not having your Web-browsing habits tracked).
- Send and receive e-mail messages or other data (e.g. credit card numbers) that will not be intercepted or read by persons other than the intended recipient(s) (Kelly and McKenzie, 2002, *Journals of Medical Internet Research*, 2002; 4(2): e12, retrieved from http://www.jmir.org/2001/2/e20).

3. THE IMPACTS OF E-HEALTH ON PATIENT'S RIGHTS OF PRIVACY

New technologies have vastly improved the ability to electronically record, store, transfer and share medical data. While these new advances have potential for improving health care delivery, they also create serious questions about who has access to this information and how it is protected. Additionally, this technology is threatened by potential unauthorized intrusion, such as computer hackers who have been known to tap illegally into private information on computer networks. Computer hackers could possibly gain access to and even alter patient records (http://www.ntia.doc.gov/reports/telemedine/privacy.htm)

As e-Health technologies and applications become more capable and potentially widespread, we must be mindful that the possibilities of increased access to healthcare services and information also bring new concerns. Among these are concerns about how we determine the quality of technology mediated care and how to manage / ensure individual privacy, access to health services, self-determination and choice. As e-Health proliferation continues, the need to determine the safety and efficacy, clinical utility, and cost-effectiveness of new e-health in relation to traditional services grows (Maddox, "retrieved from http://www.nursingworld.org/ojin/ethicol/ethics_10.htm).

Most of the recent discussions about the protection of personal information and in particular health information have focused on the impact of developments in information technology and the increasing use of computerized record systems. "The health care industry is in the midst of an era of unprecedented computerization of medical records and data." Computerizing records is part of many health care reform proposals, since it would not only increase efficiency but also significantly cut costs (Tigerstrom, "retrieved from http://www.lexis.com).

There is no doubt that "pervasive use of computers has enhanced society's ability to collect, store, retrieve, process, and disseminate data on individuals, quite often without the individual's knowledge and consent." (Tigerstrom, "retrieved from http://www.lexis.com).

The centralized storage of large amounts of information also increases the likelihood and severity of breaches of privacy. Traditionally, records have been kept in manual form in a number of different (and usually secure) locations, making it difficult to obtain information and especially to obtain and combine a wide range of data from various sources. Unless special protections are built into the system, access to a database can provide an authorized or unauthorized user with an unprecedented amount of information. Even when different sets of data are held in different systems, it is often possible to "link" or "match" the data for a particular individual using some identifier. This practice, known as computer matching, presents a serious threat to personal privacy since it allows a user to compile a detailed dossier or profile on an individual by linking data from many different sources, and thereby acquire extensive knowledge about that person, without the individual's knowledge or consent. Matching may also detach information from its context and lead to the proliferation of false or misleading information (Tigerstrom, "retrieved from http://www.lexis.com).

It is sometimes assumed that individuals who attend a health care organization thereby enter into a relationship with all the health care functionaries who work there in a way that permits everyone to access the clinical record with impunity (Magnusson, 2002, "retrieved from http://www.lexis.com).

From the discussion above we can see that besides offering many advantages, e-health also bring negative impact that is the threat against individual's privacy, especially the privacy of patients who enter to a new form of relationship with healthcare provider within e-health. In order to ensure that the customers of e-health or more specifically the patients are satisfied in entering any activities within e-health, their privacy must be protected. The question is how and to what extent individual privacy should be protected in the health care arena.

The protection to the patient's right of privacy on e-health can be done through two ways, namely ethics and laws. For the following the discussion will highlight both ethical and legal protection to the patient right of privacy.

Health law has always placed a high value on the autonomy of individual patients. Respect for the patient as an autonomous individual is also implicated in the physician's duty not to breach the confidence of her patient and the patient's ability to claim a measure of control over her own health information. The instrumental value of privacy in the health care setting involves the importance of a patient's trust in his care providers. If a patient fears disclosure of personal information, he may avoid seeking treatment or offer false information, potentially harming both his own health and that of others (Tigerstrom, "retrieved from http://www.lexis.com).

VI. CODE OF ETHIC FOR E-HEALTH

Since the creation of the Hippocratic Oath about 400 B.C., protecting the privacy of patients has been an important part of physicians' code of conduct. Over time, health information has come into use by many organizations and individuals who are not subject to medical ethics codes, including employers, insurers, government program administrators, attorneys and others. As uses of medical information multiplied, so have regulatory protections for this highly sensitive and deeply personal information.

As health information and health services become available through the internet, many new questions emerge. For instance, will e-Health services be included as part of a defined set of basic services that all peoples should have access to? What services will be covered and how will we ensure access and equitable distribution among economically disadvantaged populations? In the future, when we provide access to face-to-face health services, should we also provide access to e-Health information and services? (Maddox, "Ethics and the Brave New World of E-Health", retrieved from http://www.nursingworld.org/ojin/ethicol/ethics_10.htm).

Given concerns about access and equity concerning e-Health, a number of concerns emerge. One concern is about access and equity related to electronic health information and services on the internet. If access to such services is only available in work and public settings, will privacy and confidentiality concerns be disregarded? Will access be available when the individual is present and when the system is available for use? More importantly, because of the potentially sensitive nature of health information on the internet, access to such information at home is critical. What public concerns exist related to uneven availability of internet access? Should access to electronic health information be considered central to accessing the full array of health services in the future *(Maddox,* "Ethics and the Brave New World of E-Health", retrieved from http://www.nursingworld.org/ojin/ethicol/ethics_10.htm

To ensure online quality and privacy protection, what guidelines might a nurse consult to address these questions? What policies are needed and how should nurses advocate for them? Because the Internet is changing how people receive health information and healthcare, everyone who uses the Internet for health-related purposes must work together to create an environment of trusted relationships. Such relationships will assure quality information and services, protect privacy, and enhance the value of the Internet for both consumers and providers of health information products and services *(Maddox,* "retrieved from http://www.nursingworld.org/ojin/ethicol/ethics_10.htm.).

A number of groups (public and private) are developing quality criteria and on-line codes of conduct to help consumers understand the issue of quality and how their personal information is used by web sites. In May 2000, the Internet Healthcare Coalition's e-Health

Initiative announced the release of an international e-Health Code of Ethics. The goal of the e-Health Code of Ethics is to ensure that individuals can confidently and with full understanding of known risks realize the potential of the Internet in managing their own health and the health of those in their care. The e-Health Code of Ethics sets forth eight principles: candor, honesty, quality, informed consent, privacy, professionalism in online healthcare, responsible partnering, and accountability (Rippen & Risk, 2000).

A summary of these principles follows:

- *Candor*: Disclose information that would likely affect consumers understanding or use of the site or purchase or use of a product or service. What is disclosed should include who owns or has a major financial interest in the site, what the site's purpose is, and any relationships such as advertising partners.
- *Honesty*: Ascertain that information, including content and claims about health products, is truthful and not misleading. Distinguish content intended to promote or sell a product or service from educational and scientific content.
- *Quality*: Make good-faith efforts to evaluate information to ensure that information is consistent with the best available evidence. Specific recommendations include allowing only qualified professionals to provide personalized medical advice or care; indicate clearly whether advice is based on scientific studies, expert consensus or professional or personal experience or opinion; acknowledge that some issues are controversial (present all views); present information in easy-to-understand, user-friendly formats; and indicate what sources were used in providing information.
- *Informed consent:* Clearly disclose potential user privacy risks and keep from using personal data without the user's permission (individual consent), clearly indicate what data are being collected when users visit the site, who is collecting the data, how the site will use the data, and whether the site will share data (with whom and for what purpose).
- *Privacy*: Users have the right to expect that their personal data will be kept confidential, so e-Health sites must take reasonable steps to prevent unauthorized access to or use of personal data.
- *Professionalism in online health care*: Physicians, nurses and other health care professionals who provide specific, personal medical care or advice online should abide by the ethical codes that govern their professions. In all cases this calls for professions to do no harm, protect confidentiality, put consumers' interests first, clearly disclose sponsorships or financial incentives, clearly disclose any fees involved, and obey laws and regulations of all relevant jurisdictions. Professionals should specify their professional credentials, disclose where they practice and give clear instructions for follow-up care when appro-

priate. They also should clearly explain the constraints of online diagnosis and treatment recommendations (including explanation of when online consultation can and cannot or should not take the place of face-to-face interaction with a professional).

- *Responsible partnering*: Web sites must take reasonable efforts to make sure that sponsors or partners abide by applicable laws and uphold the same ethical standards as the sites themselves. They should insist that sponsors not only influence the way research results are displayed but also clearly indicate whether links to other sites constitute an endorsement of those sites.
- *Accountability*: Clearly indicate how users can contact the site owner or manager, provide easy-to-use tools for site visitors to give feedback, review complaints from users promptly, and encourage users to notify the site's manager if they believe partners or affiliates have violated any laws or ethical principles.

VII. THE NEED OF SPECIFIC REGULATION OF E-HEALTH

E-health occupies a space in and between the two worlds of the internet and health care, neither of which operates under clear privacy rules (Goldman and Hudson*,* 2000, " retrieved from http://www.lexis.com). In order to protect patient's right of privacy, regulations are needed, besides internal code of ethics among the participant.

Internationally, the past few decades have seen the development of standards for the protection of personal information. The right to privacy is recognized in several international agreements on human rights, including the International Covenant on Civil and Political Rights and the European Human Rights Convention (Tigerstrom, Tigerstrom, "retrieved from http://www.lexis.com).

There is no specific regulation governing the activities within e-health in Indonesia so far. However, considering that the development of information technology runs quite fast in this country, sooner or later e-health activities will become a reality in the future. Therefore a specific regulation governing such activities will be needed in order to protect mainly patient's right of privacy.

The development of the information and communication technology has changed in some extent the way to manage data. With the technology the activities on collecting, storing, and transmitting the data can be done electronically. Consequently it raises the risk of data misuse up. In order to give legal protection to personal data, there should be a specific regulation regulating that matter. As a comparison, the Malaysian Government has enacted Personal Data Protection Act. The Act is projected to serve any activities which are characterized as e-basis, such as e-banking, e-commerce and sooner or later e-health. Some materials of the bill will be discussed in the following.

The Act deals with among other things personal data. Under the Act, the term 'personal data' is defined as 'any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user including any expression of opinion about the individual and any indication of the intentions of data user in respect of that individual (Azmi, 2002) The above definition includes in its scope; any information or opinion, as long as it is identifiable to a living person; and data that is processed both manually and electronically.

VIII. CONCLUSION

From all discussions above, we can conclude that besides offering many advantages, e-health also bring negative impacts mainly the threat against individual's privacy, especially the privacy of patients who enter to a new form of relationship with healthcare provider within e-health. In order to ensure that the customers of e-health or more specifically the patients are satisfied in entering any activities within e-health, their privacy must be protected. The question is how and to what extent individual privacy should be protected in the health care arena. The protection to the patient's right of privacy on e-health can be done through two ways, namely ethics and laws.

There is no specific regulation governing the activities within e-health in Indonesia due to the fact that such activities are still limited or even have not existed yet, however, considering that the development of information technology runs quite fast in this country, sooner or later, e-health activities will become a reality in the future. Therefore a regulation specifically governing such activities will be needed in order to protect mainly the patient's right of privacy.

The development of information and communication technology in many countries has changed in some extent the way to manage data. With the technology the activities on collecting, storing, and transmitting the data can be done electronically. Consequently, it raises the risk of data misuse up. In order to give legal protection to personal data, there should be a specific regulation governing that matter in Indonesia. As a comparison, Malaysian Government proposed Personal Data Protection Bill. The Bill is projected to serve any activities which are characterized as electronic-based (e-based), such as e-banking, e-commerce and sooner or later e-health. Quoting Barbara, "much of the law on personal data is also applicable to medical information" (Tigerstrom, 1998, " retrieved from http://www.lexis.com).

BIBLIOGRAPHY

Alvarez, Richard C., "The Promise of E-Health - A Canadian Perspective", retrieved http://www.ehealthinternational.net/popups/articles/window.php.

American Telemedicine Association, 2001, "A Guide to E-Health for the Healthcare Professional: An Introduction", retrieved from http://www.atmeda.org/ehealth/guide.htm

Azmi, Ida Madieha, 2002, "E-Commerce and privacy Issues: An Analysis of the Personal Data Protection Bill", *International Review of Law Computers & Technology*, Volume 16, No.3, P.317-330.

Bennett, Belinda, "New Challenges for Old laws?" *Australian Law Journals* 2001, retrieved from http://www.lexis.com.

Eysenbach, Gunther, "What is E-Health", Journal of Medical Internet Research, retrieved from http://www.jmir.org/2001/2/e20.

Goldman, Janlori and Zoe Hudson, "Virtually Exposed: Privacy and Health", *All-Full Text Medical Journals,* November–December 2000, retrieved from http://www.lexis.com.

Goldsmith, Jeff, "Health Tracking", *All-Full Text Medical Journal*, January-February 2000, retrieved from http://www/lexis.com.

Kelly, Grant, and Bruce McKenzie, 2002, *Journals of Medical Internet Research*, 2002; 4(2): e12, retrieved from http://www.jmir.org/2001/2/e20.

Maddox, Peggy Jo, "Ethics and the Brave New World of E-Health", retrieved from http://www.nursingworld.org/ojin/ethicol/ethics_10.htm.

Malaysian Personal Data Protection Act 2005

Magnuson, Roger, 2002, "Data Linkage, Health Research and Privacy", *Australian Law Journals March,* retrieved from http://www.lexis.com.

"Privacy, Security and Confidentiality", retrieved from http://www.ntia.doc.gov/reports/telemedicine/privacy.htm.

Tigerstrom, Barbara von, 1998, "Protection of Health Information Privacy: The Challenges and Possibilities of Technology", *International Law Review* Articles, retrieved from http://www.lexis.com.