COMPUTER METHODS AND PROGRAMS IN BIOMEDICINE 82 (2006) 277–282

journal homepage: www.intl.elsevierhealth.com/journals/cmpb

Taiwan's perspective on electronic medical records' security and privacy protection: Lessons learned from HIPAA

Che-Ming Yang[a], *Herng-Ching Lin*[a], *Polun Chang*[b], *Wen-Shan Jian*[c,a,*]

[a] *Taipei Medical University School of Healthcare Administration, No. 250, Wu-Hsing Street, Taipei 110, Taiwan*
[b] *Institute of Health Information and Decision Making, National Yang Ming University, Taiwan*
[c] *Institute of Public Health, National Yang Ming University, Taiwan*

ARTICLE INFO

Article history:
Received 7 February 2006
Received in revised form
29 March 2006
Accepted 10 April 2006

Keywords:
Medical information
Electronic medical record
Security
Privacy
Protection

ABSTRACT

The protection of patients' health information is a very important concern in the information age. The purpose of this study is to ascertain what constitutes an effective legal framework in protecting both the security and privacy of health information, especially electronic medical records. All sorts of bills regarding electronic medical data protection have been proposed around the world including Health Insurance Portability and Accountability Act (HIPAA) of the U.S. The trend of a centralized bill that focuses on managing computerized health information is the part that needs our further attention. Under the sponsor of Taiwan's Department of Health (DOH), our expert panel drafted the "Medical Information Security and Privacy Protection Guidelines", which identifies nine principles and entails 12 articles, in the hope that medical organizations will have an effective reference in how to manage their medical information in a confidential and secured fashion especially in electronic transactions.

1. Introduction

There are two competing interests in maintaining medical information security and privacy: effective provision of healthcare and patient autonomy. Patient autonomy is proposed to be the current theoretical justifications for the right of privacy in medical information, because autonomy encompasses the right to control personal health; however, in order to provide effective and quality cares, the healthcare system needs sharing of medical information in a timely fashion [1]. Paperless electronic medical records have demonstrated to be able to improve clinical effectiveness [2]. With the rapid progress of computerization and electronic transactions under the National Health Insurance (NHI) scheme, people are worried about the confidentiality of their disease and health status in Taiwan.

The advancement of technology will force the legal system to adapt. The adaptation in turn feedbacks on the technical practice. All sorts of legal bills regarding electronic medical information protection have been proposed around the world including Health Insurance Portability and Accountability Act of 1996 of the U.S. (herein after HIPAA) [3], Council of Europe Committee of Ministers' Recommendation No. R (97) 5 on the Protection of Medical Data [4], Australia's Privacy Act 1988 [5] and New Zealand's Health Information Privacy Code of 1994 [6]. In Taiwan, although the Physician Act, the Medical Care Act, the Computerized Personal Information Protection Act, the Electronic Signature Act and the Criminal Code, etc., all have relevant provisions, compared with related foreign regulations, the laws and rules regarding this issue in Taiwan are more decentralized, without a single centralized law like HIPAA. Recognizing the importance of medical information

* *Corresponding author*. Tel.: +886 2 27361661x3610; fax: +886 2 23789788.
E-mail address: jj@tmu.edu.tw (W.-S. Jian).
0169-2607/$ – see front matter © 2006 Elsevier Ireland Ltd. All rights reserved.
doi:10.1016/j.cmpb.2006.04.002

privacy and security protection, the Department of Health (DOH) of Taiwan sponsored this study to further investigate the potential structure of a centralized bill that focuses on managing computerized medical information's privacy and security. The purpose of this study is to ascertain what constitutes an effective legal framework, which lives up to the expectations of healthcare professionals, medical informatics experts and the general public, in protecting both the security and privacy of health information, especially electronic medical records.

2. HIPAA and the else

HIPAA is the well-known model in this area of legal expertise. HIPAA was enacted on August 21, 1996 with the goals of "improving the portability and continuity of health insurance coverage" [3]. In order to facilitate portability, HIPAA calls for "administrative simplification", which was defined as an attempt to facilitate the electronic transmission of health information through the establishment of standards and requirements [3]. Pursuant to HIPAA's mandates, the U.S. Department of Health and Human Services (DHHS) implemented Privacy Rule, Security Rule, Transactions and Code Set Standards and Identifier Standard.HIPAA applies to health plans, health care clearinghouses and health care providers who transmit any health information in electronic form [3]. All these three constitute the "covered entities" subsequently defined in the implementing regulations, such as the Privacy Rule [7].

Health information in HIPAA means "any information, whether oral or recorded in any form or medium", that "is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and relates to the physical or mental health or condition of an individual, the provision of health care, or the payment for the provision of health care [3]. "Individually identifiable health information" is further carved out the whole picture of health information. The term "individually identifiable health information" means any health information that identifies the individual [3]. The "individually identifiable health information" is subsequently defined by DHHS as "protected health information" in the Privacy Rule [7].

There are two globally recognized principles, which are also embodied in HIPAA, in addressing health information privacy and security. First, the principle of non-disclosure is seen in HIPAA' privacy rules which states that covered entities may not use or disclose protected health information, except as permitted or required by the law [7]. Secondly, there is minimum necessary principle, which means in HIPAA when using, disclosing, or requesting protected health information, "a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request" [7].

In the Privacy Rule, the individuals have rights to access and amend the protected health information. Each individual has "the right of access to inspect and obtain a copy of protected health information about the individual in a designated record set" [7], and "the right to have a covered entity amend protected health information or a record about the individual in a designated record set" [7]. However, the covered entities can deny the individual requests and some of the protected health information are exempted from the individual's access, such as psychotherapy notes, the "information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding", and the health information subject to the protection of the Clinical Laboratory Improvements Amendments of 1988 [7]. An individual also has a right to notice the uses and disclosures of protected health information that may be made by the covered entity [7].

HIPAA requires that all covered entities that maintain or transmit health information electronically establish and maintain "reasonable and appropriate" administrative, technical and physical safeguards to ensure integrity, confidentiality and availability of the information [3]. The Secretary of DHHS shall adopt security standards that is "reasonable and appropriate" by taking into account "(i) the technical capabilities of record systems used to maintain health information; (ii) the costs of security measures; (iii) the need for training persons who have access to health information; (iv) the value of audit trails in computerized record systems; (v) the needs and capabilities of small health care providers and rural health care providers" [3].

3. The current laws and regulations in Taiwan

Although there is not yet a comprehensive and centralized set of privacy and security rules regarding health information in Taiwan, all sorts of relevant rules are scattered in various laws and regulations. For instance, the Medical Care Act states that medical organizations and their staff cannot disclose medical information acquired during practice without good causes [8]. The Physician Act [9] and other healthcare professionals' regulations state the same. The Criminal Code also punishes those, including healthcare professionals, disclose their clients' information without good causes with imprisonment up to 3 years [10]. The Electronic Signature Act deals with the security issues of all electronic transactions by creating statutory digital signature safeguards [11]. The Computerized Personal Information Protection Act is primarily concerned about privacy and governs all personal information stored in computers with a few exemptions. All personal information that is processed by computers is protected by this Act and medical information that contains personal information is not exempted [12]. Personal rights included in this Act are inquiry, copy, revision, supplement, deletion, etc. and the personal rights specified therein cannot be waived by any contract [12].

4. The effort of drafting medical information security and privacy protection guidelines in Taiwan

After thorough review of domestic and international relevant laws and regulations, we gathered multiple disciplinary experts to form a focus group in this study. The focus group consisted of medical informatics experts, clinicians, lawyers

Table 1 – The nine principles as purported in the guidelines

1. *Principle of minimum necessary*: When medical organizations or their staff collect, use, or disclose medical information, or request medical information from another organization or relevant staff member, the organization or its relevant staff must make reasonable efforts to reduce the scope of collecting, using, or disclosing the medical information to the minimum as needed
2. *Principle of direct collection*: When medical organizations or their staff collect medical information, they must do so from the patients or their legal representatives
3. *Principle of respect and notification*: When the medical organizations and their staff collect, use, or disclose medical information, they must respect the patients or their legal representatives, and be attentive of whether they are informed and voluntary
4. *Principle of equality and justice*: The medical organizations and their staff cannot use unlawful or unjust methods to collect, use, or disclose medical information
5. *Principle of compliance with current laws*: When medical organizations or their staff collect, use, or disclose medical information, they must comply with the current relevant laws and regulations
6. *Principle of maximum reasonable*: The medical organizations that store the medical information must, under reasonable limits, make the best efforts to ensure the security of medical information
7. *Principle of protection of patients' rights*: When medical organizations or their staff collect, use, or disclose medical information, they must protect patients' rights; in addition, the patients still maintain certain rights to their personal medical information stored in medical organizations
8. *Principle of non-disclosure*: Medical organizations and their staff cannot disclose any medical information without the consent of patients
9. *Principle of protection of life and public interests*: When medical organizations or their staff collect, use, or disclose medical information, they must do so in protecting life and public interests

and representatives from various professional associations and consumer organizations. We convened five plenary sessions and held numerous working group meetings in the study period. A special website for "medical information security and privacy protection" [13] was also established to serve as an on-line forum for comments and discussions by the general public.

As indicated above, the existing regulatory framework can more or less cover most of the privacy and security violation in transmitting medical information. However, the lack of a consolidated bill often makes people wonder whether they are in reality protected. A comprehensive legislative bill will take enormous amount of time to draft and pass the legislature. At present, our local expert panel advised DOH to adopt non-statutory guidelines as a gesture to the general public and the healthcare profession that the government does not turn a blind eye on this issue.

According to the consensus of our panel, the "Medical Information Security and Privacy Protection Guidelines" was drafted. The guidelines purport nine principles including minimum necessary, direct collection, respect and notification, equality and justice, compliance with current laws, maximum reasonable, protection of patients' rights, non-disclosure and protection of life and public interests (Table 1). In order to clarify how the nine principles should operate in reality, there are 12 articles in the guidelines. Article 1 defines the terms applied in the guideline (Table 2). The other 11 articles enunciate the details of the information flow from collection, creation, storage, use, authorization and disclosure in more details (Table 3).

5. The comparison between HIPAA and Taiwan's proposed guidelines

In our guideline draft, the covered entities are "medical organizations" which are defined as "the organizations where physicians practice" in Taiwan's Medical Care Act [8]. Unlike HIPAA applies to health plans, health care clearinghouses and health care providers, the scope of our covered entities is more limited. Starting from 1995, Taiwan has implemented an universal coverage health plan, i.e. NHI. There is a very limited market of private health insurance and healthcare clearing houses. Therefore, we focus on the information processes within the medical organizations, which consist of mostly hospitals and clinics. The drawback of this kind wording is that other forms of healthcare organizations, such as nursing home, are not included. The advantage is that DOH can focus their efforts in a more targeted population.

Another distinction is the scope of information encompassed. HIPAA regulates "health information", whereas our draft does "medical information". HIPAA defined "health information" as any information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse

Table 2 – Definitions of terms applied in the guidelines

Terms	Definitions
Medical information	Medical records in any form
Medical organizations	Medical organizations established in accordance with the Medical Care Act
Medical and relevant staff	Staff who are involved in or manage the patient's medical services or medical information
Collect	The process of gathering patient's related medical information by medical organizations and their staff
Create	The process of generating patient's related medical information by medical organizations and their staff
Use	Share, apply, or analyze medical information descriptively or by statistics
Disclose	The medical organizations or their staff release, transmit, offer or publish the medical information by any methods to outside parties

Table 3 – The abridged version of the 12 articles of the guidelines

Article 1	Definitions of terms
Article 2	The guidelines apply to all medical information collected by medical organizations
Article 3	The purposes of collecting medical information must comply with relevant laws and regulations and be in accordance with the principle of minimum necessary
Article 4	Medical information should be collected directly from patients as the principle
Article 5	Medical information can only be collected after the patients or their legal representatives, spouses, relatives, or related persons have been informed
Article 6	The methods of collecting medical information must be lawful, fair and just
Article 7	The medical organizations or their medical and relevant staff that create and store medical information must ensure the maximal data security to a reasonable extent
Article 8	Patients should be guaranteed rights to review and duplicate medical information
Article 9	The storage of medical information must comply with the laws and regulations
Article 10	The privilege and scope of using medical information must comply with the principle of minimum necessary
Article 11	The disclosure of medical information must be consistent with the purposes of storage and the principle of minimum necessary
Article 12	The medical organizations and their medical and relevant staff cannot disclose medical information without proper reasons

relates to the physical or mental health of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual. Our definition of medical information is "medical records". "Medical records" are elaborated in the Medical Care Act [8] to include physician records, examination and laboratory reports and records created by other healthcare professionals while practicing. This approach corresponds to our choice in covered entities. We leave the health information which circulates outside of medical organizations out of the realm of the guidelines. Aside from the fact of a single payer system in Taiwan, we also consider the reality that there is jurisdictional limitation of DOH, and we can simply form consensus in a targeted population, i.e. medical organizations, and govern the information contained therein.

What is worth mentioning is that our definition of medical information does not only encompass computerized medical records but also medical records stored in any medium. This definition was purposefully adopted to circumvent the misunderstanding that medical information stored in non-electronic media is not accorded the same level of protection. This approach is also in keeping with the revision proposed by Taiwan's Executive Yuan to change the Computerized Personal Information Protection Act to the Personal Information Protection Act so as to extend the scope of protection to non-computerized personal information [14]. Nonetheless, there is obviously less and less non-computerized medical information down the road.

HIPAA and its implementing regulations establish a category of protected health information that denotes individually identifiable health information. We purposefully leave out the term "protected information" in order to avoid causing the confusion that only some information is protected and the rest is not. Our basic stance is that all medical information is protected and can be used by all medical and relevant staff with access privilege control. The use and disclosure of medical information has to be in line with minimum necessary principle all the time. All medical and relevant staff within the medical organization can use health information so long as in consistence with minimum necessary principle. In addition, under the non-disclosure principle, the medical organizations and their staff can only disclose to outsiders under the following exceptions: disclose to the patient or his/her legal representatives; under emergency disclose to the patient's spouse, relatives, or related persons; disclose to the governmental authorities when requested; to comply with other mandatory requirements; for the sake of protecting life and public interests. Therefore, the exchanges among various organizations always require patients' authorization in principle. Only de-identified information can be freely disclosed. The de-identified medical information can be disclosed without patients' consent or authorization. HIPAA specifies the identifiers of the individual or of relatives, employers, or household members of the individual, that have to be removed in order to become de-identified [7]. Our guidelines also left out these specifications on purpose in order to avoid the problem of thoroughness and cumbersomeness at this stage.

For research purposes, if the patients' identities have to be included in the processes, patients' identities can be disclosed to the researchers without authorization from the patients so long as the research project has gained the approval of research committees of respective medical organizations. The researchers who are in possession of the not de-identified medical information also have the fiduciary duty of confidentiality and can only publish the data with de-identified information according to Article 10. This design is to avoid undue hindrance to scientific researches and accord due respect to the operation of institutional review boards.

HIPAA adopted a reasonable appropriate safety standard in the area of security. Our guidelines opt for a maximum reasonable safety principle. What is reasonable? According to the definition of the Merriam-Webster dictionary, reasonable means "not extreme or excessive" [15]. Therefore, a reasonable safety measure should be an appropriate one. Reasonableness appears to be the prevailing test for all standards. For instance, it has been argued that HIPAA and the related rules fail to specify how to determine what amounts to minimum necessary, and hence the covered entities should be held to a reasonableness test [16]. Our expert panel felt that we had to send out a stronger signal to our target audience in order to arouse their awareness of the importance of medical information security. Therefore, we did not reiterate the "reasonable appropriate" language of HIPAA and enunciated a new "maximum reasonable" principle. What we are trying to convey here is that the general public expect medical organizations to maintain maximal information security. The issue of accountability can also be taken care of under this notion, since we require privilege control for all accesses within the organizations. However, the

expert panel was not unmindful of the practical difficulty in establishing security measures, such as cost and technical feasibility. Whether it is maximal can be ascertained from the perspective of whether it is reasonable. It is generally recognized that protection of privacy and security can be best done together [17]. Therefore, by insisting on maximal security in protecting medical information, medical organizations can provide their patients with maximal privacy protection.

We identified patients' right in our draft as the counter part of HIPAA's individual's right. In our patients' rights, patients can access, copy, supplement and make inquiries about their medical information. We did not explicitly permit patients to amend or delete medical information. We deliberately avoid the word "amend" to circumvent the difficulty that patients will constantly ask the medical staff to change the records which they do not like, such as history of sexually transmitted diseases or psychiatric disorders. Under current wording, patients can ask the medical organizations to put in any statement made by themselves into their medical records as a "supplement" without changing the original records. However, this effort creates a conflict between our guidelines and the Computerized Personal Information Protection Act. As illustrated before, non-waivable personal rights in the Computerized Personal Information Protection Act include deletion and medical information is not exempted from that Act. Nonetheless, we are concerned about the implications if patients can delete their information from their medical records at will. Free deletion will make medical records unreliable and affect healthcare professionals' behavior. If the right to delete is to be withheld from the personal rights granted in the Computerized Personal Information Protection Act, a statutory exemption will have to be created in the future.

Unlike HIPAA, there are no exemptions or protected areas in the medical records, which the patients cannot put their hands on in our guidelines. According to HIPAA, some of the protected health information are exempted from the individual's access, such as psychotherapy notes, the information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative proceeding, and the information subject to the protection of other laws [7]. This kind of work product doctrine does not work any more in Taiwan. The 2004 amendment of Medical Care Act granted patients right to request a complete photocopy of individual medical records from medical organizations [8]. Before the enactment of this amendment, patients were only entitled to medical record summaries by law. Medical organizations can decide on their own as to whether patients could have a full copy of their medical records or part of them. Due to the general public's outcry for full accesses to individual medical records, DOH yielded to the pressure and there was no work product exemption in medical records from then on.

There is no right to notice under our draft. Since we allow free flow of information within the medical organization and deny outbound flow unless explicit authorization from the patients with some exceptions, notices will come from the patients in the form of consent not from the organizations. There is no right to accounting of disclosures of protected health information, either. According to HIPAA, an individual has the right to receive an accounting of disclosures of protected health information made by a covered entity in the 6 years prior to the date on which the accounting is requested [7]. This has been described to be the most onerous requirement of HIPAA and will deter covered entities from releasing their medical records for research [18]. Therefore, we entrust the institutional review boards to do their jobs and did not impose this burden on medical organizations in our guidelines.

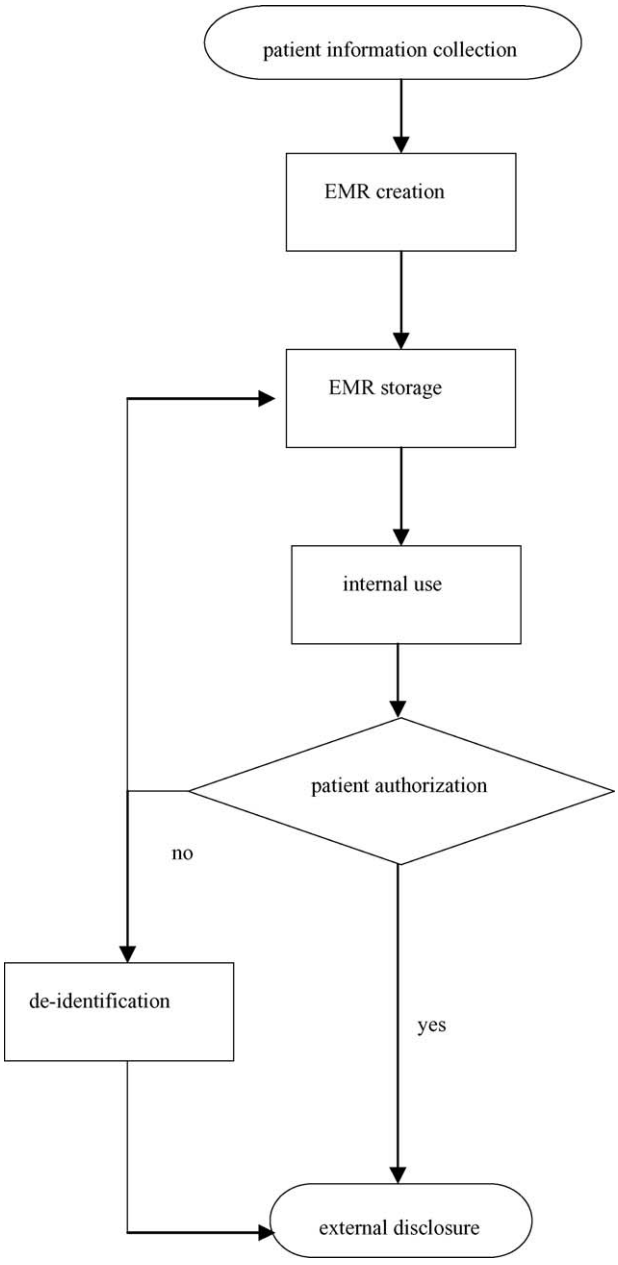

Fig. 1 – The electronic medical record (EMR) process defined in the guidelines.

In summary, from the perspective of electronic medical record programming, our guidelines separate the electronic medical record process into collection, creation, storage, use and disclosure (Fig. 1). There is no need to obtain authorization from patients for use, and yet disclosure will need authorization with only a few exceptions. The whole computerized system will have to meet the minimum necessary

and maximal security standards in each step to a reasonable extent.

Undoubtedly, what do and do not come into the guidelines will have a profound impact on medical informatics standards. For instance, immediately after the passage of HIPAA, the Healthcare Informatics Standards Board of American National Standards Institute started compiling health data standards in order to map the standards into the requirements of HIPAA [19]. The extent of impact on medical informatics standards in Taiwan the proposed guidelines would have remains to be seen.

6. Conclusion

Medical information security and privacy is a very complicated issue, which deserves much legal and technical attention. Under the sponsor of DOH, our expert panel drafted the "Medical Information Security and Privacy Protection Guidelines". The draft proposes nine principles and 12 articles, which catches up with international legislative trends without violating domestic laws. We intend the guidelines to serve as a policy directive at present rather than an iron fist regulation. Therefore, the principles have incorporated major medical ethics concerns, such as the principle of autonomy and respect for patients, etc. By so doing, we believe these guidelines constitute an effective legal framework that can serve as an useful reference for the rest of the world in protecting both the security and privacy of health information, especially electronic medical records. We expect privacy protection and medical information security can be strengthened by the spontaneous efforts of medical organizations after the announcement of the guidelines in the near future. Although the guideline draft is the consensus of our study, we anticipate that more controversies will surface in subsequent legislative or administrative proceedings, and how to achieve minimum necessary and maximal security to a reasonable extent will be the focus of great debate in implementing electronic medical records.

Acknowledgements

This study was funded by the grant (No. 93-5021) from the Executive Yuan of Taiwan. We especially appreciate the assistance of the Information Center of DOH, Taiwan Association for Medical Informatics, and the experts and representatives who participated in our research efforts.

REFERENCES

[1] P.I. Carter, Health information privacy: can congress protect confidential medical information in the "information age?", William Mitchell Law Rev. 25 (1999) 223–286.
[2] C. Dobbing, Paperless practice-electronic medical records at Island Health, Comput. Methods Programs Biomed. 64 (2001) 197–199.
[3] Health Insurance Portability and Accountability Act of 1996 (U.S.), Pub. L. No. 104-191, 110 Stat. 1936 (codified in scattered sections of U.S.C.).
[4] Council of Europe Committee of Ministers, Recommendation No. R (97) 5, of the Committee of Ministers to Member States on the Protection of Medical Data (adopted by the Committee of Ministers on 13 February 1997 at the 584th meeting of the Ministers' Deputies).
[5] Australia Act No. 119 of 1988 as amended, incorporating amendments up to Act No. 49 of 2004.
[6] New Zealand Health Information Privacy Code of 1994 as amended, incorporating amendments up to Amendment No. 5, commenced 30 July 2002.
[7] Code of Federal Regulations (U.S.), Title 45, Part 160.
[8] Medical Care Act (Taiwan), incorporating amendments commenced 5 February 2005.
[9] Physician Act (Taiwan), incorporating amendments commenced 16 January 2002.
[10] Criminal Code (Taiwan), incorporating amendments commenced 2 February 2005.
[11] Electronic Signature Act (Taiwan), incorporating amendments commenced 14 November 2001.
[12] Computerized Personal Information Act (Taiwan), incorporating amendments commenced 11 August 1995.
[13] http://privacy.doh.gov.tw.
[14] Personal Information Act Bill (Taiwan), ratified by the Executive Yuan in February 2005. pending legislation.
[15] http://www.webster.com/dictionary/reasonable, accessed at 2005/12/23.
[16] P.D. Jacobson, Medical records and HIPAA: is it too late to protect privacy? Minn. Law Rev' 86 (2002) 1497–1514.
[17] P.P. Swire, L.B. Steinfeld, Security and privacy after September 11: the healthcare example, Minn. Law Rev. 86 (2002) 1515–1540.
[18] M.L. Durham, How research will adapt to HIPAA: A view from within the healthcare delivery system, Am. J. Law Med. 28 (2002) 491–502.
[19] J.M. Fitzmaurice, A new twist in US health care data standards development: adoption of electronic health care transactions standards for administrative simplification, Int. J. Med. Inform. 48 (1998) 19–28.