Study on Applying ISO/DIS 27799 to Medical Industry's ISMS

[1] Kwo-Jean Farn, [1,2]Jiann-Ming Hwang, [1]Shu-Kuo Lin
[1]Institute of Information Management, National Chiao Tung University, Taiwan
[2] Computer Science & Information Engineering, Ming Chuan University, Taiwan

Abstract: At present, as medical care sites use more and more IT system, information systems have come to play an important role in the business operation of medical organizations. It is an important goal for management at medical organization in Taiwan to keep the security of medical informatics. HIPAA had been run about ten years in USA, thought its efficiency has still remained to be seen, HIPAA has become the benchmark of the information governance in the information security of medical industry. The Department of Health of Taiwan had adapted from HIPAA and issued the HISPP/GD that included 9 principles and 12 articles altogether. This text will probe into the ISO/DIS 27799, the feasibility of applying it to the management of domestic medical organization and the corresponding detail of ISMS. By this way, we hope that Taiwan's medical organization can build a medical information system and manageable environment that according with the security requirements of confidentiality, integrality and availability.

Key-Words: CNS, HIPAA, HISPP/GD, Risk Appetite, Information Governance, Health Information Security, Information Security Management System (ISMS).

1 Introduction

In January 2001, the "Information & Communication Security Mechanism Plan" was approved in Council Meeting No.2718, and the "National Information and Communication Security Taskforce" (NICST) was established, to actively launch Taiwan's information & communication security infrastructure. After that, the certification of ISMS has already become the priority of information security in Taiwan. On the basis of cooperating with the demand for mutual trust among medical health organ, relevant enterprise's partner and patient, the first two parties must look for the solution to offer the securities of information, trade and communication, and control all information materials correlated with the patient.

However, many medical organizations do not handle personal information such as patients' medical care data as systematically as they do risk management for mistakes in medical practice. In addition, as medical care sites use more and more IT system, information systems have come to play an important role in the business operation of medical organ. Since the shutdown of an information system would seriously affect medical services, controls are also required to deal with this. If information security cannot be maintained, many disadvantages will follow. Security management is vital if these disadvantages are to be addressed.

ISO/DIS 27799 (Security management in health using ISO/IEC 17799) is drafted by ISO Technical Committee 215 (Health Informatics Working Group) in autumn of 2003 and under ballot as a Draft International Standard; ballot closes in October of 2006. It is based on BS-7799-2(CNS17800), ISO TR13335, and ISO/IEC17799-2000. Its main content is to apply ISMS to the management of medical information and to implement the medical security system with ISO/IEC 17799. Comparing to HIPAA, the domestic HISPP/GD has less contents, has not included the technical aspect, and has only the effect of promotion. In our opinion, the mentioned ISO/DIS 27799(announced by ISO), CNS 17799:2006 (issued by BSMI, Taiwan) CNS 27001:2006 and other standards altogether can be regard as foundation of improvement and revision on HISPP/GD [Fig. 1].

The rest of this paper is organized into four sections. Section 2 states the adaptation of HIPPA. In section 3 and 4, applying ISO/DIS 27799 to medical information security and related issues are discussed. In section 5, conclusion will be addressed.

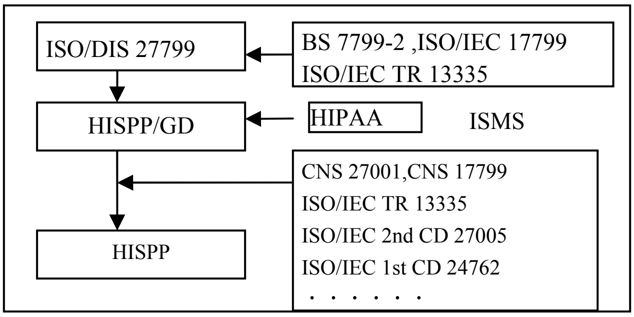


Fig. 1: Applying ISMS to HISPP/GD

Note:
(1) CNS (Chinese National Standards. administered by the Bureau of Standards, Metrology and Inspection (BSMI) of the Ministry of Economic Affair(M.O.E.A),Taiwan)
(2) HISPP/GD (Heath Informatics Security and Privacy Protection guideline draft, Taiwan)

2 Reference of HIPAA

The e-Taiwan Program is divided into 5 major parts: Infrastructure, e-Society, e-Industry, e-Government and e-Opportunity. The e-Taiwan Program is revised and evaluated regularly according to changing needs. E-Society promotes online education, entertainment, culture, health care, and transportation services, these initiatives will improve the quality of services available to the public. HIPAA is adapted as the reference for creating the HISPP/GD that is an objective of e-health service inside the e-Society program.

For the purpose of the regulation of information security and confidentiality and according with the requirement of privacy, the Health Insurance Portability and Accountability Act (HIPAA) is enacted by the U.S. Congress in 1996. HIPAA states the security mechanism for information system as follows: (a) administrative procedure; (b) physical safeguards; (c) technical security services; (d) technical security mechanisms. Comparing to HIPAA, the domestic HISPP/GD is less complex, only consider to strength the security control of medical informatics and patient's privacy protection in Taiwan's medical organization. Thought its contents is very different from the regulation of HIPAA, the HISPP/GD still keeps the relevant spiritual intension of HIPAA, such as the principle of minimum requirement that when medical organ collecting the patient's information should obey the rule of minimum necessary requirement as not to collect information other than medical usage. It also offer some other articles that according with the improvement of current Taiwan's medical society, such as the maximum security in reasonable scope principle for executing reference, because there is no definite standard for security, and it impossible to ask medical organ to unlimitedly budget for security, but only can ask them to evaluate security needs depending on their budget.

In October 2001, Legislative Yuan of Taiwan passes three readings of the Digital Signatures Law, providing a legal basis for domestic e-commerce development and electronic information exchange. NHI (National Health Insurance) IC card that has the fundamental data and partial medical records of the patient, can be the media of communicating and exchanging of medical informatics. By combining NHI IC card with the standard of HL7 (Health Layer 7) and DICOM (Digital Image Communication in Medicine), various kinds of medical information can circulate smoothly among the medical organizations. The doctor uses medical personnel card, the patient uses NHI IC card and with the professional qualification authentication of the medical organ, this triple safety measures, can fill a guarantee that the privacy of patient's medical information is protected and communication security is safe. Under this situation, doctor and nursing staff use the computer properly, while carrying out the diagnosis and treatment they can quickly grasp patient's health status, understand the previous therapy situation and disease that patients suffering from. By this way they can avoid repeatedly examining, checking, and using medicine and get the result of economizing medical resources.

For the purpose of information security and protection, while considering the construction of the structure of "medical informatics security policy", medical organization should base on the angles of structural and responsible aspect so as to build the fundamental layers of legal, organization, function, medical treatment, privacy, society, ethics and technology; and consider such directions as integrality, validity and accountability. By August 4, 2006, there have 94 private and public organizations in Taiwan passed the ISMS certification, but till November 30, 2006, still very few organizations have put "ISMS policy" in their ISMS document. In considering the ISMS policy of the "medical informatics security policy", medical organization should to set up and include both the "ISMS policy" and "medical informatics security policy"; In other words, ISMS should include "information security policy" and "ISMS policy"" at the same time.

3 ISO/DIS 27799

The ISO/DIS 27799(Draft International Standard) excerpts the controls from ISO/IEC 17799, its main content is to apply ISMS to the management of medical information and to implement the medical security system using ISO/IEC 17799. The following sections will narrate the steps and methods of how to construct and apply ISMS system to medical informatics security (MIS), the content of ISO/DIS 27799 that relative to the essentiality of MIS and the management of MIS, and the relevant weakness, threat, risk assessment and risk management of MIS.

3.1 Essentials of MIS and Its Management

One of the important points when managing information security is to clarify "the purpose for which the MIS is being performed." It is important to define the objectives of MIS clearly, and manage security to achieve those objectives. The following are examples of some of the more important objectives: (1) Protecting Personal Information; (2) Preventing Mistakes in Medical Practice; (3)

Maintaining the Functions of the Medical Organs (The Continuity of Medical Services). The roles of medical organizations become greater in a major disaster. Even if the social infrastructure has suffered enormous damage, they must recover quickly and continue to provide medical services. They must also put in place suitable defensive measures to handle malicious attacks, to deal with problems such as cyberterrorism [15].

3.2 Risk Management of MIS

Factors that cause risks are called "threats." More specifically, a threat is "a potential factor that causes a contingency that may result in loss of or damage to information assets or damage to the organization." A threat only becomes a problem when it has been occurred and has factors that cause actual damage. The weaknesses of the information assets that may elicit threats are called "vulnerabilities."; the vulnerability itself will not become a problem. A risk may be elicited by combining threats and vulnerabilities. The following Assets: information, people (knowledge), physical, software and services, must been protected for information security.

Risk prevention means preventative measures that prevent a risk from occurring and is therefore especially effective for risks that cannot easily be dealt with via financial compensation. For example, it is easy to insure against credit cards forgery, but the large amount of damage caused by a leak of personal information (especially medical information) is difficult to cover with insurance alone. Measures for dealing with risks as follows: (a) Risk control: Using controls that help actively minimize damage. (b)Risk transfer: Measures to transfer risks to another company, e.g. by contract. (c)Risk retention: Measures for accepting risks as an organization (d) Risk avoidance: Measures taken if no appropriate measures are found.

Emergence operation is critical for the patient's life, any disorder in the security or management of the back-up information system will cause disaster that causing death, losing of trust and brand image and causing claims for compensation. In the damage or risk analysis, the following three types are most fundamental: (a) potential damage type - such as earthquake, arson, etc. and evaluating the degree of causing possibility and severity approximately; (b) impact degree of the damage - such as number of death, the amount of property loss; (c) response control – while aiming at the frequency and the severity of impact about damage, the constructed preparedness or responding strategy. In addition to obeying the general medical operation requirement, medical organ should implement risk assessment regularly in order to controlling the occurring possibility of risk to acceptable range.

Table 1 Examples of the look-up score table of information assets

Information Assets	Threats								
	1			2			3		
	Vulnerabilities								
	1	2	3	1	2	3	1	2	3
1	░ 1	░ 2	░ 3	░ 2	░ 4	░ 6	░ 3	░ 6	▓ 9
2	░ 2	░ 4	░ 6	░ 4	░ 8	▓ 12	░ 6	▓ 12	▓ 18
3	░ 3	░ 6	▓ 9	░ 6	▓ 12	▓ 18	░ 8	▓ 18	▓ 27
4	░ 4	░ 8	▓ 12	░ 8	▓ 16	▓ 24	▓ 12	▓ 24	▓ 36
░	Range in which risks are acceptable (<9)								
▓	Range in which action should be taken to deal with the risk (>=9)								

While practicing the risk assessment of emergence center, we can produce an evaluation score table of risk matrix [Table 1] by following information: (a) the occurring possibility of the accident; (b) the impact (people, assets, business, preparedness, the internal and external responses, etc.); (c) threat, vulnerability and risk of information security. There are many methods for calculating the risk value. If we set the acceptable (negligible) risk value as less than 9, then the darker area in Table 1 represents the unacceptable risk situation that the medical organ must to do some prevention control before accident happenings so as to control the occurring possibility of risks to acceptable range.

4 Building the ISMS System of Medical Informatics Security

ISO/DIS 27799 is based on BS-7799-2(CNS17800), ISO TR13335, and ISO/IEC17799-2000. It builds the ISMS System of medical informatics by using the process model of PDCA (Plan-Do-Check-Act), as showed in Fig.3. The implementation detail is in the reference [1-3]. The system of medical security management, for example, managing problems with medical services, is built on the PDCA cycle.

4.1 PCDA Process Model of ISMS

CNS 27001:2005-10-15 is the improvement and update of CNS17800 (BS7799-2:2002), the digest of change for building and managing ISMS is as the following requirements: (1) The organization shall define the scope and boundaries of the ISMS and state the details and justification. (2)The ISMS policy is considered as a superset of the information security policy. These policies can be described in one document. (3)The risk assessment methodology selected shall ensure that risk assessments produce comparable and reproducible results. (4)Controls objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process. This selection shall take account of the criteria for accepting risks as well as legal, regulatory and contractual requirements. (5)Define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results. (6)Monitor and review the ISMS should have the functionality as to help detect security events and thereby prevent security incidents by the use of indicators. (7)Measure the effectiveness of controls to verify that security requirements have been met. (8)Review risk assessments at planned intervals and review the level of residual risk and identified acceptable risk, taking into account changes to effectiveness of the implemented controls. (9)Update security plans to take into account the findings of monitoring and reviewing activities

One of the advantages of establishing ISMS is that security measures can be carried out with certainty. For achieving the objects of ISMS, this improvement is a part of the Act-Improvement process in the PDCA cycle. It is important to continue to improve the effectiveness of the ISMS using the information security policy, information security goals, the results of audits, analysis of monitored events, corrective and preventive action and the output from management reviews.

The "internal audits" control of ISO/DIS 27799 has been included in its "management reviews" section; we suggest that the "internal audits" control should be operated independently as in CNS 27001. The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS: conform to the requirements of this International Standard and relevant legislation or regulations; conform to the identified information security requirements; are effectively implemented and maintained; and perform as expected [1]. If nonconformities related to the way the ISMS is implemented or operated are found from the results of an audit and management review, actions must be taken to remove the causes of nonconformities and prevent them from reoccurring.

As the idiom says "well begun is half done." The organization shall establish, implement, operate, monitor, review, maintain and improve documented ISMS within the context of the organization's overall business activities and the risks they face [2].

In medical organizations, there is the risk that any problem caused by a personal information leak or an error handling the information or information systems may become a problem for society. It is important to identify possible nonconformities and their causes earlier to take preventive action. When establishing ISMS in an organization, it is necessary to bear in mind that the management process should include a function for identifying changes to risk due to conditions and environmental changes, and a function for learning from cases of trouble, and trouble in other organizations, so that preventive action can be taken in management reviews.

4.2 ISMS Policy and Risk Appetite

"It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process and subsequently back to the ISMS policy and objectives." is the requirement stated in section 4.3.1 of CNS 27001 [ISO/IEC 27001:2005(E)]. Based on that, the core of ISMS policy is located in the veining of the context of risk management and risk assessment, as showed in Fig. 4 and Fig. 5 [1-4, 6, 13, and 14]. The ISMS is a system for all industries, always facing uncertainty. When management trying hard to create the value of information security for their stakeholder, the challenge is dependent on how high the uncertainty that he/she will accepts. Uncertainty means risk or cost; the value of organization may be raising or falling because of it. The risk management of ISMS makes management to deal with uncertainty and the related risk and cost effectively, and let the organ to boost their ability of creating the value of managed information security.

ISMS is operated in a changing environment of globalization, technology, organization, production, competition, regulation, and enactment. These factors cause the uncertainty of ISMS. Uncertainty could come from the happening possibility in the future or the unknown result of an event/accident; or could come from the strategic selection of the ISMS policy; Such as the schedule and percent of the construction of DiD (Defense in Depth) [17], the requirement of "The Freedom of Information Law" and "Personal Data Protection Law", change of legislation etc. It will influence the strategic selection of the ISMS policy and create the relative risk and cost. Management use strategy to calibrate the risk appetite of organization and make it the same as the needs of organization [6].

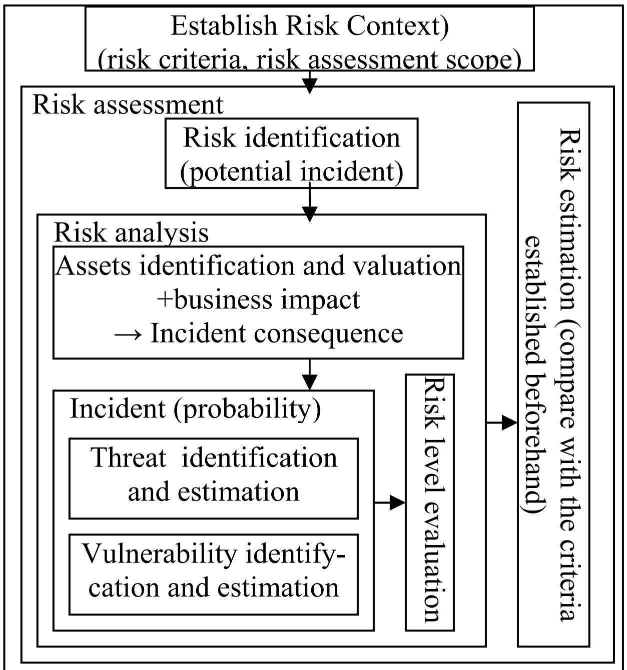
Information security policy offers the necessary reliable foundation for the management and audit of

ISMS; promotes more concernment and avoids the potential problems while implementing ISMS. The effectiveness of ISMS also involves the following topic: organization's business, operation threat and technical framework [12, 14, and 17].

Ensuring continuous management commitment is essential for accepting the structural processes of ISMS. Personnel need to recognize information security control and know how to do it, and to understand the benefit that this control will bring to organization. Generally speaking, unless supported by management, ISMS will be unsuccessful by itself. The Effectiveness measurements and indicators of ISMS provide the risk image of critical issue [Figure. 6], let management to accept this concept and let organization willing to commit for supporting and maintaining ISMS. ISMS policy provides the implementation objectives for the effectiveness measurements and indicators of risk communication, risk monitor and risk review of the ISMS as stated in Table3. Table 4 is the illustration of the retained reserves in Table 3. In sum of above, while organization is pursuing its mission or vision, the philosophy of considering its risk management and building its ISMS policy is depending on how much of risk the organ shall or willing to accept and how to alignment the strategic risk management context of the organization, In other words, under the same information security policy, an organization with different risk management philosophy, its ISMS policy and the retained reserves of its risk management sub-plan will be different.

5 Conclusion

Security is like air, valueless in the beginning but becoming valuable while suffering from and losing it. The leak of privacy information causes unparalleled threat to Digital-Taiwan Program; time -consuming in verification, difficult in assessment, while ordinary becoming unusual, we shall recognize how to ensure the achievement of information security assurance that using the following method: "Information Operations (IO) that protect and defend information and information systems by ensuring their confidentiality, availability, non-repudiation, authentication, and integrity, this includes providing for restoration of information systems by detection, incorporation protection, and reaction capabilities." is important segment of constructing the information security infrastructure of Digital-Taiwan, and is valuable public wealth.


Establish Risk Context)
(risk criteria, risk assessment scope)
Risk assessment
Risk identification
(potential incident)
Risk analysis
Assets identification and valuation
+business impact
→ Incident consequence
Incident (probability)
Threat identification and estimation
Vulnerability identify-cation and estimation
Risk level evaluation
Risk estimation (compare with the criteria established beforehand)

Source:Dr Elzbizta Andrukiewicz , (co-editor of ISO/IEC27005), Importance of Risk management, Presentation to the ISO/IEC JTC/ SC27 Security Workshop, 2005-23-06.

Fig. 5: Image of Risk assessment process based on ISO/IEC 27005: 2007? (under development)

The target of ISMS is "To Ensure the access of information resource is legal, to offer complete, uninterrupted operation of information system, in any stage that is possible for information attack." The security of information system is like a chain; its strength is depending on its weakest link. As showed in Fig. 7, the combination of information security policy, information security issue policy (Ex.: privacy policy), information system security policy (Ex. access control policy) and ISMS policy is the real source pool for hardening ISMS strength.

Based on CNS 27001:2006, CNS 17799:2006 and ISO/DIS 27799 and referenced on HIPAA, This paper probes into suggestion of the update and improvement of the HISPP/GD in Taiwan, and statement how to apply ISMS to medical informatics management and how to implement medical informatics security system. We deeply hope that this work will be some help to the management and security of medical informatics and let the people in Taiwan have better medical service and life.

(NOTES: Owing to the page limitation, Fig. 4: Risk management process based on ISO/IEC 27005 and ISO/IEC 18045 and Table 3: Communication, monitor and review of risk management have been omitted)

Consequence	Risk distribution		
Very serious	A2,C2	C1,L3,I1	I2,R1
Serious	L2	R2,A3	I3
Unserious	R2,L1	A1	C3
	Almost impossible	Possible probility	Almost sure

Fig. 6: Image of information security risk context
L= Legal or Regulatory environment, I =Integrity
R= Reliability, A=Availability, C=Confidentiality.

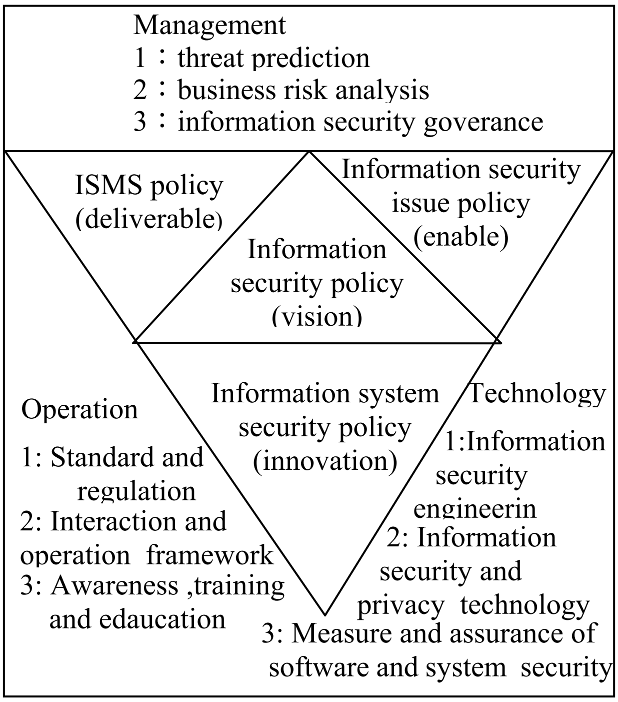

Management
1 : threat prediction
2 : business risk analysis
3 : information security goverance
ISMS policy (deliverable)
Information security issue policy (enable)
Information security policy (vision)
Operation
1: Standard and regulation
2: Interaction and operation framework
3: Awareness ,training and edaucation
Information system security policy (innovation)
Technology
1:Information security engineerin
2: Information security and privacy technology
3: Measure and assurance of software and system security

Fig. 7: ISMS Set framework

Table 4: Cost of ISMS risk management sub-plan

	Risk type	Risk process cost type
ISMS risk management sub-plan	known	corrective action
		preventive action
	unknown (including risk retention)	retained reserves
Source: A guide to project management body of knowledge, 2000 ed., PMI and this study		

References:

[1] BSMI-MOEA, ROC, *Information technology - Security techniques-Information security management systems - Requirements*, CNS 27001:2006.

[2] BSMI-MOEA, ROC, *Information technology — Security techniques — Code of practice for information security management,* CNS 17799 :2006.

[3] BSMI-MOEA, ROC, *Information Security Management Manual (draft)*, 2006.

[4] BSMI-MOEA, ROC, *The guideline for Risk Management, Vocabulary, standard usage,* CNS 14889:2005。

[5] BSMI-MOEA, ROC, *Information technology — Security techniques — Code for information security management*, CNS 17800:2002。

[6] COSO, *Enterprise Risk Management*, 2004.

[7] Department of Health- Executive Yuan, ROC. *Heath Informatics Security and Privacy Protection guideline draft*, http://www.cdrs.org.tw/news_4 /medinfopriv.doc,2004.

[8] Farn K.J., Lin Shu-Kuo, Lo Chi-Chun., *Study on ISMS Foundation Courses for Auditors?* WSEAS TRANSACTIONS on INFORMATION SCIENCE AND APPLICATIONS, Issue 10, Volume 3, pp. 1955 ~ 1962, 2006.

[9] Farn K.J., Lin Shu-Kuo, Lo Chi-Chun ., *Study on the Network Isolation Security Requirements for Cyber Space?* WSEAS TRANSACTIONS on COMPUTERS, Vol.5, No.5, pp.1034~1040, 2006.

[10] Farn K.J., Fan H.C., Lin Shu-Kuo, *A study on the certification standard of Information Security Management System--Information Security Policy and Information Security system Policy,* Information Security comunication,Vol.13, No.1, 2006, pp.163- 176.

[11] Farn K.J., *Information Security Policy and Information Security system Policy (reference data)*, The Chinese Cryptology and Information Security Association, 2006.

[12] Howard, M. & D. Le Blanc, *Writing Secure Code* 2nd ed, Microsoft Press. 2004

[13] ISO, I*nformation technology - software life cycle processes - Risk management*, ISO/IEC 16085: 2004(E).

[14] ISO, *SSE--CMM* ®, ISO/IEC 21827: 2002(E).

[15] JIPDEC, *ISMS User' s Guide for Medical Organizations*, JIPDEC, pp1-77. 2004

[16] Kevin Beaver, Rebecca Herold, *The Practical Guide to HIPAA Peivacy and Security Compliance*, Auerbach Publications, 2004.

[17] NSA (2002), *Information Assurance Technical Framework*, Release 3.1, 2002.

[18] Research, Development and Evaluation Commission-Executive Yuan, ROC, *Risk Management Operation Manual*, 2005

[19] Sheldon Borkin, *The HIPAA Final Security Standards and ISO/IEC 17799*, SANS Institute. 2003.

[20] U.S.104th Congress, *Health Insurance Portability and Accountability Act*, Public Law 104-191, Aug.21, 1996.