Information Security Guidelines for Healthcare Institutions

Chao-Ming Chen
Institute of Healthcare Information Management
National Chung Cheng University, Taiwan
168,University Rd, Min-Hsiung Chia-Yi, Taiwan, R.O.C.
TEL: 886-5-2721500 FAX: 886-5-2721501
u8824341@yahoo.com.tw

Abstract: In recent years, the form of medical records already slowly changed from paper form to electronic form. The new information science and technology makes the transmission of information easier and convenient. On the other hand, the exposedness of individual privacy and information secret would be too difficult to keep and the use of new science and technology has increased the risk of information leakiness.

The information security problem appears slowly in the electronic medical record. People that are indiscreet and negligent could cause improper damage to the information management. For this reason, the security guidelines could help healthcare institutions to improve insider and outsider security problem. The security guidelines should refer to BS7799 and HIPAA that we would take many advantages. Finally, we must estimate the benefit from purchase, integration, management, operations, maintenance, time lost, clumsy interfaces and procedures etc. These may spend a lot memory and time, so we should evaluate the cost and risk of BS7799 and HIPAA in each item; it could help us to guide how to select low cost, low risk and high benefits standard item to create the security guidelines.

Keywords: Internet Security and Privacy.

Introduction

The Information System in 21 th already to become the hospital essential tool, specially may increase efficiency of information system and reduce the cost.. However, the computerization of health information, while offering new opportunities to improve and streamline the healthcare delivery system, also presents new challenges to security problems and individual privacy interests in personal healthcare data [4].And The medical record exchange and the share has hastened for the current situation, grows the security problem which comes, creates patient's privacy and individual data enormous threat .Patient's data has the high sensitivity, most did not hope has a mind the public figure to the data exchange when is carried on revises correct or steals, perhaps in exchange process because controls the tube not when creates the internal outside the data to release. .In health care, because of these security risks and the uncertainty of security requirements in electronic networks, providers often discourage the use of electronic networks for the transmission of most patient data and other sensitive information [1], [7].

Recognizing the potential dangers to computerized patient information, Congress mandated the implementation of system security standards through the Health Insurance Portability and Accountability Act [(HIPAA) Public Law 104–191], requiring the adoption of security standards that take into account the technical capabilities of record systems used to maintain health information [4].So we ready need a guidelines that told Hospital's high level manager how to control risk、risk management、security plan….because all most managements have not any idea to security for Hospitals, if Manager have a security guideline , could help them to make security plan、control Risk and Risk management. But the security standards like BS7799 or HIPAA have too many control objectives that hospitals could not implement all control objectives. Because of the most hospitals resources is limited.

Threats of Health Care Information

According to Daniel P. Lorence and Richard Churchill 's research that paper-base of Healthcare Institutions could provide more security more than computer-base of Healthcare Institutions.

This is because Healthcare Institutions even have a lot of security problem in paper base work. And what's security problem are in our Healthcare Institutions. The consensus among health care CIOs is that the most important threats to patient information confidentiality are the following Table 1[9]:

Table1

Threats
1.From inside the patient care institution : *Accidental disclosures*. *Insider curiosity*. *Insider subornation*. **2.From within secondary user settings**
3.Outsider intrusion into medical information systems

Table 1 show we the threats all most come from Insider of Healthcare Institutions So Healthcare Institutions must

Proceedings of the Fifth International Conference on Electronic Business, Hong Kong, December 5-9, 2005, pp. 448 - 451.

have the better internal control mechanism.

BS7799 and HIPAA

The BS 7799 Code of Practice is intended for use as a reference document by managers and other persons responsible for the information security within an organization. It is intended as a standard for the management of information security rather than for the practice of information security itself. In other words, it does not set out to be a technical manual but rather describes the sorts of controls that should be in place and how they should be managed. It may be regarded as a basis upon which to build a security policy but is not meant to be a definitive list of the measures that should be in place in every organization.[8]. Common is suitable each industrial BS7799, because the Healthcare Institutions has its industrial characteristic, specially in organization surface, therefore should join following several projects to take the thanking improvement the goal.[10]：

1. Medical records protections stipulation, maintains the patient‘s privacy not to violate.
2. The patient‘s information security rights, stated and protection patients the right which goes see a doctor in the hospital.
3. Outside of hospitals the use patients data, outside the hospital organization or the unit request obtains patients data, should request to observe stipulation the hospital correlation.
4. Medical records storage, guarantees patients medical record storage the security.

The right of privacy speaking of sickness is extremely important, specially in the nowadays democracy social privacy is current the important subject which takes, studies according to Cai Chia Ting [2] pointed out 95% managers of Healthcare Institutions all thought the medical information security and the privacy are the present hospital management important topic. Especially in data exchange or share time we must need to consider the secure question. But based on the Healthcare Institutions characteristic should hold the privacy to patient information, the security, and the secret and so on the characteristic, this also is several important ideas which in HIPPA emphasized, especially on Healthcare Institutions.

What Kind of Assets Need to Protect.

The common information system security Threats has following several kind of like Table 2。all Healthcare Institutions must be select some important controls to protect because they resources is limit. Many organizations have developed information systems for the collection and storage of patient data, but do not adopt corresponding security committees or teams, nor security manager/officers or coordinators According to Daniel P. Lorence and Richard Churchill[3]

Table 2 [6]

Natural and political disasters	Fire or excessive heat、Floods、Earthquakes、High winds、War and terrorist attack。
Software errors and equipment malfunction	Hardware or software failures. Software errors or bugs Operating system crashes. Power outages and fluctuations. Undetected data transmission errors.
Unintentional acts	Accidents caused by: Human carelessness Failure to follow established procedures Poorly trained or supervised personnel Innocent errors or omissions. Lost, destroyed, or misplaced data. Logic errors.
Intentional acts (fraud & computer crime)	Sabotage Computer fraud Misrepresentation, false use, or unauthorized disclosure of data. Misappropriation of assets. Financial statement fraud.

How Analyzes the Information Security Weakness.

The BS 7799-2 specifies requirements for establishing, i mplementing and documenting information security man agement systems (ISMSs). It specifies requirements for security controls to be implemented according to the ne eds of individual organization.

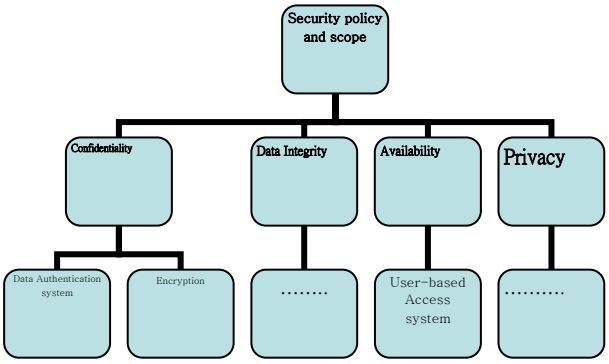
How to Establishing a Management Framework

The information safety control because HIPAA has considers the right of privacy protection the part, therefore uses HIPAA to discover the healing institute the item which must pay attention regarding the information security, finally coordinates the item which the electronic medical record clearing house must pay attention, and weakness which possibly can have on the present domestic electron medical record safe exchange overhead construction proposes the suggestion method. Must be able to complete the information to be safe first must finish the information security the management, first should appraise each control goal with can accept the risk which the risk and possibly can have, second is the selectivity control goal and reduces the risk to the scope which can accept, third avoids the risk and the shift risk arrives the third party, suggests the method, fourth carries on the safe plan which explained on front the development and the thorough execution and the revision, this for the information security and flow of and the executive program the internal control necessity, its specify and the method as follows explained: [5]

1. **Define the information security policy and the scope of the information security management system：**

First must look according to, security, the secret, uniformity major term and so on private dense launches lists our system scope and information security policy. Figure 1 shows an

example tree that the information security policy and the scope of the information security management system could be defined by the tree. We could List Confidentiality、Data Integrity、Availability and Privacy in the parent and we could list detail items in the subtree. That several information system needs to protect. appraised each control goal with can accept the risk which the risk and possibly can have: We want to decide on the protection policy which the medical record exchange security needs, and discovers the scope and the project which the electronic medical record exchange the system must protect, and appraised its risk with the resources which must consume, because resources limited, we are impossible to various information property all to make the consummation the protection, has the risk regarding each kind of possibility which the risk all must perform to calculate possibly occurs to have high.



2. **Risk assessment and management：**

selectivity controls goal and reduces the risk to the scope which can accept: This time must after various information property appraise grades makes the different rank in view of the different information property the protection, receives in view of the goal which must control carries on the security aspect the disposition and the tube controls, falls the risk the degree which can accept to us, exchanges by the electronic medical record said regarding the information bank protection, the material protection is count for much, may prepare under the enough resources situation as soon as to prepare in addition helps the main engine to carry on the backup the movement, can largely reduce the risk, and falls the risk which the information bank material drains to fall to the scope which may accept.

We should have clearly to know in the organization in this stage the material flow. The convention the organization of inside of the expert conference to obey HIPAA and the BS7799's control items confirm decides the important degree, and then List all of the control items in the checking table.(ex table 3). A score is determined for each alternative. The perfect alternative has a score of 1.0. The score for an alternative always lies between 0 and 1.0 and each score is determined independently of the scores of the other alternatives. Alternatives with identical scores are considered tied or equally close-to-perfect in the evaluation.

The weights to be used for the criteria, sub-criteria,and the intensity levels at each level of the tree using pairwise comparisons are determined.Let C(i,j) be a pairwise comparison that the decision-maker makes between two elements i and j,which are children of a node in the AHP tree(the children are also nodes in the AHP tree). Each pairwise comparison can be interpreted as a ratio scale . For elements i and j on the same level of the tree, C(i,j) can be interpreted as follows:[5]

$$Cij = \frac{\text{The weight the decision-maker would like to assign to element i}}{\text{The weight the decision-maker would like to assign to element j.}} \quad (1)$$

$$\text{weight} = \frac{1}{\sum row(i)} \quad (2).$$

Table3

	Outpatient System	Hospitalization System
Outpatient System	1	2
hospitalization System	1/2	1
weight	0.67	0.333

We could assign the information security of budget according to on table weight. Achieves most has the benefit the resource distribution and using the company information assignment, this uses above the information security, without the capital original assignment is insufficient.

3. avoids the risk and the shift risk to the third party:

We may the risk which may estimate avoid letting he occur, perhaps the risk by way of insurance giving to the insurance company which insures.

4. **The Security plan development:**

Finally we had to defer to a moment ago the risk height different project, started with organization resources how many to carry on the safe plan the plan and the development.

5. **Implementation**:

Carried on according to the information security plan content safely controls the tube, including organization's resources AND-OPERATION flow control, and the explicit definition power and responsibility, had the flaw regarding the process in which occurred to be supposed to record, then will be allowed to develop the security plan to take the improvement in the future the basis.

The conclusion

Security takes the degree on the present healing institute to the information not to be high, although knew has the information security but not to know how does, now this research specially chooses the electronic medical record material to exchange this subject, hoped can impel the electronic medical record exchange while the government

also to consider the information peaceful comprehensive thing, this research thought the information security and the electronic medical record material exchange is a body, is does not have the means to cut, therefore this research showed the information securityty control process, because the information security control is the information security basic condition, after achieves the information security control the request, the healing institute only then has the ability reference, This research establishment information security direction and composition. Healing institute's information is security also in the start stage, but also has quite many subjects not to have the means to make the detailed discussion in this research, why like does the healing institute affect the security the factor? The influence has in a big way? The risk has high? How deals with these security issues the countermeasure is what? ... And so on all is the quite interesting subject, might take the futurology subject the reference.

References

[1] A. Dwivedi, R. K. Bali, M. A. Belsis, R. G. Naguib, and N. S. Nassar,"Toward a practical healthcare information security model for healthcareinstitutions," in Proc. IEEE Int. Conf. Information Technology Applicationsin Biomedicine, 2003, pp. 114–117.

[2] Cai Chia Ting, Wang Dawei, Guo Hsusung, Legislation of and the practice research the Taiwan medical service information security - to impels feasibility of the HIPAA from the capital method experience, 2001。

[3] Daniel P. Lorence and Richard Churchill ,Incremental Adoption of Information Security in Health-Care Organizations: Implications for Document Management, IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE, VOL. 9, NO. 2, JUNE 2005

[4]. Office of Technology Assessment, Protecting Privacyin Computerized Medical Information, report for US Congress,OTA-TCT-576, September 1997.

[4] "Health Insurance Portability and Accountability Act of 1996," 104th Congress, Public Law 104-191, 1996.

[5] LAWRENCE D. BODIN, LAWRENCE A. GORDON,and MARTIN P. LOEB,Evaluating Information Security Investments Using the ANALYTIC HIERARCHY PROCESS, COMMUNICATIONS OF THE ACM February 2005/Vol. 48, No. 2.

[6] Marshall B.Romney、Pai John Steinbart,Accounting Information Systems , 2006.

[7] R. Falk, "Health care privacy: Preparing for the brave new world," J.Med. Practice Management, vol. 17, no. 1, pp. 35–36, 2001.

[8] Tony Elbra.,A MANAGEMENT GUIDE TO BS 7799 ,1999

[9] Washington, DC,National Research Council. For the Record: Protecting ElectronicHealth Information. National Academy Press, 1997.

[10] Ye XiangYu, , The National Yang-Ming University, utilizes the BS 7799 examinations healing institutes information security control work document,2002.