Original Article

Healthc Inform Res. 2010 June;16(2):89-99.
doi: 10.4258/hir.2010.16.2.89
pISSN 2093-3681 • eISSN 2093-369X

HIR
Healthcare Informatics Research

Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds

Woo-Sung Park, MD, PhD[1], Sun-Won Seo, PhD[2], Seung-Sik Son, BS[3], Mee-Jeong Lee, MD[1], Shin-Hyo Kim, MS[4], Eun-Mi Choi, PhD[5], Ji-Eon Bang, BS[2], Yea-Eun Kim, BS[2], Ok-Nam Kim, PhD[6]

[1]Department of Pediatrics, College of Medicine, Dankook University; [2]Department of Medical Information, Dankook University Hospital, Cheonan; [3]Hyundai Information Technology, Seoul; [4]Electronic and Telecommunications Research Institute, Daejeon; [5]Department of Healthcare Management, Kwandong University, Gangneung; [6]Department of Prevention Medicine, School of Medicine, The Catholic University of Korea, Seoul, Korea

Objectives: The information security management systems (ISMS) of 5 hospitals with more than 500 beds were evaluated with regards to the level of information security, management, and physical and technical aspects so that we might make recommendations on information security and security countermeasures which meet both international standards and the needs of individual hospitals. **Methods:** The ISMS check-list derived from international/domestic standards was distributed to each hospital to complete and the staff of each hospital was interviewed. Information Security Indicator and Information Security Values were used to estimate the present security levels and evaluate the application of each hospital's current system. **Results:** With regard to the moderate clause of the ISMS, the hospitals were determined to be in compliance. The most vulnerable clause was asset management, in particular, information asset classification guidelines. The clauses of information security incident management and business continuity management were deemed necessary for the establishment of successful ISMS. **Conclusions:** The level of current ISMS in the hospitals evaluated was determined to be insufficient. Establishment of adequate ISMS is necessary to ensure patient privacy and the safe use of medical records for various purposes. Implementation of ISMS which meet international standards with a long-term and comprehensive perspective is of prime importance. To reflect the requirements of the varied interests of medical staff, consumers, and institutions, the establishment of political support is essential to create suitable hospital ISMS.

Keywords: Information Security Management System, Information Security, Personal Health Information Protection, Security Requirements

Received for review: May 4, 2010
Accepted for publication: July 1, 2010

Corresponding Author
Sun-Won Seo, PhD
Department of Medical Information, Dankook University Hospital, Anseo-dong, Dongnam-gu, Cheonan 330-715, Korea. Tel: +82-41-550-6870, Fax: +82-41-550-6879, E-mail: swseo@dkuh.co.kr

I. Introduction

With the processing of social information management, information collection, analysis and applications are becoming the important assets which determine the competition of individuals and institutes. There are much public investments on human resource training and research and development based on enhancement in order to control the side effects of social information management [1]. As hospitals collect, use, and store personal information and health information related an individual's privacy directly, the risks of information leakage, forgery, and falsification are more serious than

any other institutions [2]. The actions for personal health information protection are very important to both hospitals and patients. To ensure the confidentiality of medical information is a fundamental condition for continuity of medical practice. So, hospitals should show reliability to patients that hospitals collect, use, disclose, and store personal health information safely according to the rules, regulations and medical laws [3]. Domestic hospitals protect personal health information through the 'Medical Service Act', 'The Act on the Protection of Personal Information Maintained by Public Institutions', and 'The Act on Promotion of Information and Communications Network Utilization and Information Protection', etc. However it is applicable only for some medical service staffs and it does not cover all staffs using medical information systems in hospitals. Also, it is not sufficient to meet the public requests of information protection.

To meet requirements of information security, hospitals should build up and implement the Information Security Management System (ISMS). It ensures the stability and reliability of information assets in hospitals and guarantees confidentiality, integrity and availability of medical information [4-7]. However, there is an absence of standardized ISMS which reflects the characteristics of medical service, so it is difficult to apply existed ISMS to medical information system. There could be serious risks related to information security and damage to both medical centers and patients. Therefore standards in a national level related to personal health information protection and security is needed to establish security in hospitals immediately.

In this paper, we recommend the standards on personal health information protection and security countermeasures which is fit for international standards and the needs of hospitals after investigating the ISMS of 5 hospitals which contain over 500 beds, based on present laws and guidelines for information security management in physical and technical aspects.

II. Methods

For the study, five hospitals which contained over 500 beds were investigated, that is, two public hospitals and three private hospitals. Three of them used electronic medical record systems, and the other two hospitals used hybrid medical record systems.

Check-lists to investigate the ISMS were designed according to international standards ISO/IEC 27001; 17799, JIS Q 15001 in Japan and the ISMS presented by the Korean Internet & Security Agency in Korea [4-7].

The check-lists were distributed to each hospitals to fill in, we interviewed the staffs directly according to the check-list terms.

Table 1. Information security indicator

Weight (score)	Yes	Partial	No
High (3)	3	2 or 1	0
Medium (2)	2	1	0
Low (1)	1	1	0

Information Security Indicator (ISI) = value of weight x value of result; Information Security Value (ISV) = average index of ISI in a detailed category.

		Score	Present codition			Plan for appication				
Control	Score high: 3 middle: 2 low: 1	Estimated score	Weight (high/ middle/ low)	Application (Y/N/P, N/A)	Evidence	Applicability (1-5)	Plan for application (Y/N)	Time to apply	Expercted problem manpower, cost)	Expercted expendit ure
1. Security policy										
1.1 Medical information security policy										
1.1.1 Medical information security policy document										
An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.	7									
1) A definition of information security, its overall objectives and scope and the importance of security as an	2									
2) A statement of management intent, supporting the goals and principles of information security in line with the	1									
3) The information security policy reviewed by related department	2									
3) Reviewed information security policy approved by owner	2									

Figure 1. Check list sample.

doi: 10.4258/hir.2010.16.2.89

Each check list term and category assessed 3 answers which were 'Yes', 'Partial', and 'No' to estimate the Information Security Indicator (ISI) and Information Security Values (ISV) (Table 1). Weight such as 'High', 'Medium', or 'Low' shows the importance of a detailed category, and 'Yes', 'Partial', or 'No' show how much they keep a detailed category. To understand realistic and practical views on information security, the plan for application was checked in applicability, application schedule (Yes/No) and expenditure terms (Figure 1).

III. Results

1. The Medical Information Security Policy

Hospitals should equip detailed information security policy and review it regularly to support for information security. As shown in Table 2, the average percentage of scores for the medical information security policy, control for information security policy documents, and information security policy maintenance and management was 53.5%, 60.0%, and 35.6% respectively. Though there were basic policy documents of information security policies required by assessments of medical institutions, there were not detailed information security policy documents.

2. The Organization of Information Security

To manage ISMS in hospitals, the organizations with assigned roles and responsibilities are needed for information security and co-ordinate each other. Table 3 showed the average percentage of scores for the organization of information security, control for internal organizations, and external parties which were 63.0%, 57.7%, and 69.2% respectively.

Table 2. Medical information security policy

Control	Score	A	B	C	D	E	Average (%)
Medical information security policy	34	14	27	26	19	5	53.5
Information security policy document	25	14	20	20	16	5	60.0
Policy approval	7	6	5	5	6	0	62.9
Policy system	14	4	11	11	6	3	50.0
Policy publish and notice	4	4	4	4	4	2	90.0
Information security policy maintenance and management	9	0	7	6	3	0	35.6
Review and evaluation	9	0	7	6	3	0	35.6

Table 3. Organization of information security

Control	Score	A	B	C	D	E	Average (%)
Organization of information security	81	40	62	54	25	74	63.0
Internal organization	44	19	37	27	4	40	57.7
Management commitment to information security	7	4	5	5	0	5	54.3
Information security co-ordination	7	0	4	4	2	7	48.6
Allocation of information security responsibilities	9	8	8	3	0	9	62.2
Authorization process for information processing facilities	6	2	6	6	2	6	73.3
Confidentiality agreements	5	4	4	4	0	4	64.0
Contact with authorities	4	1	4	4	0	4	65.0
Contact with special interest groups	2	0	2	1	0	1	40.0
Independent review of information security	4	0	4	0	0	4	40.0
External parties	37	21	25	27	21	34	69.2
Identification of risks related to external parties	6	4	1	4	4	6	63.3
Addressing security when dealing with customers	10	10	9	7	0	10	72.0
Addressing security in third party agreements	13	5	9	10	11	13	73.9
Third party security management	8	2	6	6	6	5	62.5

The level of sub-control for contact with special interest groups and independent review of information security was low (40.0%). Only 1 hospital had organization and personnel in charge of information security. Though there was a dual role for information security without exclusive charge, there were no regulations for responsibilities and roles in hospitals. In matters of the external parties' security, sub-control for third party security management and identification of risks related to external parties. It was found to be insufficient. 1 hospital did not address security with customers.

3. Asset Management

To control and maintain protection of the information asset, information asset classification which is a basic for identifying information assets and evaluating risks is needed. The average percentage of scores for asset management, control for responsibility for assets, and information classification were 32.7%, 31.6%, and 34.3% respectively. Asset management was analyzed to be the most vulnerable clause in the ISMS. There were little classification guidelines which was a base for establishment of countermeasures for information security management in hospitals. It was insufficient in making and managing the inventory of assets in hospitals. Ownerships of assets were the most inadequate among sub-controls in asset management, 4 hospitals got 0 points out of 4 in the ownership of assets clause. There were no designated

Table 4. Asset management

Control	Score	A	B	C	D	E	Average (%)
Asset management	33	4	17	6	17	10	32.7
Responsibility for assets	19	3	11	1	10	5	31.6
Inventory of assets	13	3	6	0	8	4	32.3
Ownership of assets	4	0	3	0	0	0	15.0
Acceptable use of assets	2	0	2	1	2	1	60.0
Information classification	14	1	6	5	7	5	34.3
Classification guidelines	7	0	0	2	7	0	25.7
Information labeling and handling	7	1	6	3	0	5	42.9

Table 5. Human resources security

Control	Score	A	B	C	D	E	Average (%)
Human resources security	76	52	54	41	54	34	61.8
Prior to employment	19	7	12	12	10	9	52.6
Roles and responsibilities	8	1	5	6	4	2	45.0
Screening	7	5	5	5	5	7	77.1
Terms and conditions of employment	4	1	2	1	1	0	25.0
During employment	13	12	9	13	10	3	72.3
Management responsibilities	7	6	3	7	4	0	57.1
Disciplinary process	6	6	6	6	6	3	90.0
Termination or change of employment	23	15	20	16	18	11	69.6
Termination or change of employment procedure	5	0	2	0	0	3	20.0
Return of assets	10	7	10	8	10	3	76.0
Removal of access rights	8	8	8	8	8	5	92.5
Information security education and training	21	18	13	0	16	11	55.2
Education and training plan	5	5	4	0	5	4	72.0
Education and training target	5	4	3	0	5	3	60.0
Education and training contents	6	5	4	0	4	4	56.7
Education and training evaluation	5	4	2	0	2	0	32.0

doi: 10.4258/hir.2010.16.2.89

asset managers. Only 1 hospital had ownership of assets. The level of classification guidelines, information labeling and handling was insufficient as shown in Table 4.

4. Human Resources Security

People involved in hospitals such as employees, contractors and third party user should understand the responsibilities of information protection, and hospitals should set up procedures of termination or change of employment, and the education and evaluation schedules to train all staff. The average percentage of scores for human resources security was 61.8% as shown in Table 5, among the controls, 'prior to employment' received the lowest score (52.8%). Checking consideration prior to employment, screening policy was implemented moderately (77.1%), but sub-control for roles and responsibilities, terms and conditions for employment were not at a high level. In case of termination or change of employment, 4 hospitals fulfilled the sub-control for return of assets and removal of access rights, but there were few standard procedures of termination or change of employment. Information security education and training plans were established in 4 hospitals, but no detailed target and contents. Some hospitals implemented information security education and training, which was not based on a specific plan.

5. Physical and Environmental Security

To avoid inappropriate physical access, secure areas should be defined and specified, and disposal and re-use of equipment, removal of property, and security of equipment off-premises should be prescribed. The average percentage of score for physical and environmental security, control for secure areas, and equipment security was 69.1%, 52.8%, and 82.2% respectively as shown in Table 6. The Sub-control for physical security perimeter and physical entry controls received under half score (50%). There were no entry logs of offices, even in the data processing department with concentrated information assets. Public access, and delivery showed to be the most vulnerable among sub-controls (23.3%). The level of equipment security was relatively higher than other controls and cabling security was managed well in the 5 hospitals. But equipment that could contain personal health information was disposed and re-used inappropriately.

6. The Communications and Operations Management

To ensure secure operation of medical information system, countermeasures and operating procedure should be established in accordance to information technology trends such as mobile codes. The average percentage of scores for the communications and operations management was 62.1% as shown in Table 7. The most vulnerable control was the third party service delivery which showed 35.8%. Information back-up was at a moderate level, but monitoring, media han-

Table 6. Physical and environmental security

Control	Score	A	B	C	D	E	Average (%)
Physical and environmental security	81	41	67	65	47	60	69.1
Secure areas	36	8	26	24	15	22	52.8
Physical security perimeter	9	1	7	6	2	6	48.9
Physical entry controls	9	0	8	4	2	5	42.2
Securing offices, rooms and facilities	3	0	2	3	2	2	60.0
Protecting against external and environmental threats	5	5	4	5	5	4	92.0
Working in secure areas	4	2	4	3	3	3	75.0
Public access, delivery and loading areas	6	0	1	3	1	2	23.3
Equipment security	45	33	41	41	32	38	82.2
Equipment siting and protection	8	6	8	8	6	6	85.0
Supporting utilities	11	11	10	11	9	11	94.6
Cabling security	6	6	5	6	4	4	100.0
Equipment maintenance	4	3	4	4	4	4	95.0
Security of equipment off-premises	5	4	3	3	3	3	64.0
Secure disposal or re-use of equipment	5	3	5	3	3	3	68.0
Removal of property	7	0	6	6	3	7	62.9

Table 7. Communications and operations management

Control	Score	A	B	C	D	E	Average (%)
Communications and operations management	222	130	132	171	88	168	62.1
Operational procedures and responsibilities	34	25	25	28	14	24	68.2
Documented operating procedures	8	7	7	7	5	5	77.5
Change management	12	11	10	9	2	7	65.0
Segregation of duties	3	2	0	3	3	3	73.3
Separation of development, test and operational facilities	11	5	8	9	4	9	63.6
Third party service delivery management	19	7	3	13	0	11	35.8
Service delivery	3	0	3	3	0	0	40.0
Monitoring and review of third party services	7	0	0	3	0	4	20.0
Managing changes to third party services	9	7	0	7	0	7	46.7
System planning and acceptance	21	21	19	19	8	20	82.9
Capacity management	9	9	9	7	8	8	91.1
System acceptance	12	12	10	12	0	12	76.7
Protection against malicious and mobile code	14	9	5	10	9	10	61.4
Controls against malicious code	14	9	5	10	9	10	61.4
Back-up	11	9	9	9	8	9	80.0
Information back-up	11	9	9	9	8	9	80.0
Network security management	13	0	8	11	8	13	61.5
Network controls	7	0	4	7	2	7	57.1
Security of network services	6	0	4	4	6	6	66.7
Media handling	32	17	27	24	3	25	60.0
Management of removable media	9	0	5	4	0	9	40.0
Disposal of media	9	7	6	5	0	9	60.0
Information handling procedures	12	9	13	12	3	6	71.7
Security of system documentation	2	1	3	3	0	1	80.0
Exchange of information	44	30	20	39	13	40	64.6
Information exchange policies and procedures	24	6	0	14	6	20	38.3
Exchange agreements	21	8	0	5	N/A	N/A	20.7
Physical media in transit	5	4	5	4	N/A	N/A	86.7
Electronic commerce	6	3	3	4	2	6	60.0
Security of information system	14	9	12	12	5	14	74.3
Monitoring	34	12	16	18	25	16	51.2
Audit logging	6	5	6	6	0	4	70.0
Monitoring system use	7	2	2	2	7	5	51.4
Protection of log information	6	0	1	5	3	0	30.0
Administrator and operator logs	8	0	3	0	8	0	27.5
Fault logging	4	2	2	2	4	4	70.0
Clock synchronization	3	3	2	3	3	3	93.3

dling protection against malicious and mobile codes were insufficient. In operational procedures and responsibility, the network security management of medical information system which contains very important information was not controlled. There was a lack of awareness on security vulnerability about mobile codes such as Active-X and media

 doi: 10.4258/hir.2010.16.2.89

Table 8. Access control

Control	Score	A	B	C	D	E	Average (%)
Access control	175	87	125	153	117	118	68.6
Business requirement for access control	19	11	13	14	11	13	65.3
Access control policy	19	11	13	14	11	13	65.3
User access management	44	27	23	34	30	29	65.0
User registration	14	11	14	10	10	11	80.0
Privilege management	9	5	0	9	8	7	64.4
User password management	11	5	9	7	2	5	50.9
Review of user access rights	10	6	0	8	10	6	60.0
User responsibilities	30	10	19	24	11	14	52.0
Password use	17	10	13	12	7	8	58.8
Unattended user equipment	6	0	2	6	4	1	43.3
Clear desk and clear screen policy	7	0	4	6	0	5	42.9
Network access control	27	5	21	19	18	24	64.4
Policy on use of network services	6	5	6	6	6	6	96.7
User authentication for external connections	6	0	4	2	N/A	6	40.0
Equipment identification in networks	2	0	2	1	1	2	60.0
Remote diagnostic and configuration port protection	1	0	1		1	1	60.0
Segregation in networks	2	0	2	2	2	1	70.0
Network connection control	8	0	4	6	6	6	55.0
Network routing control	2	0	2	2	2	2	80.0
Operating system access control	42	31	24	38	39	26	75.2
Secure log-on procedures	11	4	5	13	12	8	76.4
User identification and authentication	3	3	2	3	3	3	93.3
Password management system	15	12	15	11	12	11	81.3
Use of system utilities	8	12	0	9	11	3	87.5
Session time-out	2	0	2	2	1	1	60.0
Limitation of connection time	3	0	0	0	0	0	0.0
Application and information access control	11	3	7	11	8	10	70.9
Information access restriction	9	3	5	9	8	8	73.3
Sensitive system isolation	2	0	2	2	0	2	60.0
Mobile computing and teleworking	23	0	18	13	0	2	47.0
Mobile computing and communications	2	0	0	1	0	2	30.0
Teleworking	21	N/A	18	12	N/A	N/A	71.5

handling. Especially the management of removable media was not managed properly. For monitoring, clock synchronization was managed well, but the level of administrator and operator logs and protection of log information was low.

7. Access Control

To avoid control unauthorized access and control access authority to information, access control should be equipped. The average percentage of scores for access control, control for mobile computing, teleworking and user responsibilities were 68.6%, 47.0%, and 52.0% respectively which was not at a sufficient level compared to other the controls category (Table 8). Access control should be set up with identifying information and risks about business programs and analyzing security requirements. However the hospitals did not prepare the regulations and guidelines for these things. Med-

Table 9. Information systems acquisition, development and maintenance

Control	Score	A	B	C	D	E	Average (%)
Information systems acquisition, development and maintenance	158	78	133	122	79	108	65.8
Security requirements of information systems	3	3	2	3	0	0	53.3
Security requirements analysis and specification	3	3	2	3	0	0	53.3
Correct processing in applications	31	25	31	27	6	30	76.8
Input data validation	7	6	7	4	2	6	71.4
Control of internal processing	10	9	10	10	4	10	86.0
Message integrity	3	0	3	3	0	3	60.0
Output data validation	11	10	11	10	N/A	11	76.4
Cryptographic controls	21	0	13	15	14	10	49.5
Policy on the use of cryptographic controls	6	0	0	5	2	4	36.7
Network encryption	4	0	2	0	1	0	15.0
Key management	11	0	11	10	11	6	69.1
Security of system files	34	14	26	22	8	29	58.2
Control of operational software	13	10	13	11	6	11	78.5
Protection of system test data	8	0	2	5	N/A	8	37.5
Access control to program source code	13	4	11	6	2	10	50.8
Security in development and support processes	53	34	48	40	37	39	74.7
Change control procedures	19	13	19	16	16	19	87.4
Technical review of applications after operating system changes	7	7	7	1	7	0	62.9
Restrictions on changes to software packages	7	2	7	5	7	0	60.0
Information leakage	8	0	5	7	7	8	67.5
Outsourced software development	12	12	10	11	N/A	12	75.0
Technical vulnerability management	16	2	13	15	14	0	55.0
Control of technical vulnerabilities	16	2	13	15	14	0	55.0

Table 10. Information security incident management

Control	Score	A	B	C	D	E	Average (%)
Information security incident management	36	8	21	17	8	8	34.4
Establishment of security incident action system	13	0	10	8	0	0	27.7
Establishment action plan and system	13	0	10	8	0	0	27.7
Security incident action and follow-up	23	8	11	9	8	8	38.3
Reporting information security events	8	4	7	4	4	4	57.5
Reporting security weaknesses	4	4	0	3	4	4	75.0
Collection of evidence and recovery	6	0	1	2	0	0	10.0
Follow-up security events	5	0	3	0	0	0	12.0

ical information system including important personal health information should be separated from the internet, but some hospital did not separate personal medical records from networks either physically or logically. In matters of mobile computing and teleworking, there were many demands for telemedicine, but it was not allowed because of security even now.

 doi: 10.4258/hir.2010.16.2.89

Table 11. Business continuity management

Control	Score	A	B	C	D	E	Average (%)
Business continuity management	26	5	21	23	5	5	45.4
Information security aspects of business continuity management	26	5	21	23	5	5	45.4
Including information security in the business continuity management process	10	4	9	9	4	4	60.0
Business continuity and risk assessment	3	1	2	2	1	1	46.7
Developing and implementing continuity plans including information security	4	0	2	4	0	0	30.0
Business continuity planning framework	4	0	3	3	0	0	30.0
Testing, maintaining and reassessing business continuity plans	5	0	5	5	0	0	40.0

Table 12. Compliance

Control	Score	A	B	C	D	E	Average (%)
Compliance	56	36	44	44	36	36	70.0
Compliance with legal requirements	38	27	33	31	27	27	76.3
Identification of applicable legislation	3	3	3	2	3	3	93.3
Intellectual property rights	15	6	11	10	6	6	52.0
Protection of organizational records	7	6	7	7	6	6	91.4
Data protection and privacy of personal information	9	9	9	9	9	9	100.0
Prevention of misuse of information processing facilities	4	3	3	3	3	3	75.0
Regulation of cryptographic controls	2		2	2	2	2	80.0
Compliance with security policies and standards, and technical compliance	7	3	4	7	3	3	57.1
Compliance with security policies and standards	4	3	4	4	3	3	85.0
Technical compliance checking	3	0	0	3	0	0	20.0
Information systems audit considerations	11	6	7	6	6	6	56.4
Information systems audit plan	7	3	5	3	3	3	48.6
Information systems audit result and follow-up	4	3	2	3	3	3	70.0

8. Information Systems Acquisition, Development and Maintenance

Security is the integral part of information system, so security requirements should be verified each step like information system acquisition, development and maintenance. As shown in Table 9, the average percentage of scores for information systems acquisition, development and maintenance, control for cryptographic controls, and security requirements of information systems were 65.8%, 49.5%, and 53.3% respectively. Technical vulnerability management percentage was 55.0%. Only 2 hospitals reviewed security requirements in case of information systems acquisition and development. Network encryption was not applicable. Test data containing patient`s personal health information were used for information systems acquisition, development and change, and it was not reviewed appropriately.

9. Information Security Incident Management

Management of information security is need for managing information security event and problems related to information system. The average percentage of scores for information security incident management, control for Establishment of security incident action system, security incident action and follow-ups were 34.4%, 27.7%, and 38.3% respectively. For the cases of information security incident, organization systems or procedures, no actions were set up. Reporting security weaknesses was implemented in 4 hospitals, the collection of evidence and recovery and follow-up security events were at a very low level (10 to 12%) as shown in Table 10.

10. Business Continuity Management

To protect interruptions to business activities, hospitals should manage business continuity. The average percentage

of scores for business continuity management was 45.4%. Some hospitals had disastrous recovery systems, but developing and implementing continuity plans including information security, Business continuity planning framework and Testing, maintaining and reassessing business continuity plans were not established properly to face the disasters (Table 11).

11. Compliance

For compliance, hospital should review the exited law and regulation on information security. The average percentage of scores for compliance, control for compliance with legal requirements, compliance with security policies and standards, and technical compliance, and Information systems audit considerations were 70.0%, 76.3%, 57.1% and 56.4% respectively as shown in Table 12. The compliance with legal requirements, sub-control identification of applicable legislations, protection of organizational records, data protection and privacy of personal information were at moderate levels, but intellectual property rights (IPR) especially, IPR management of software was inadequate. Compliance with security policies and standards should be reviewed regularly, but regulations or guidelines for checking technical compliance did not exist. Information systems audit results and follow-ups were implemented, but the information systems audit plan was at a low level.

IV. Discussion

The aim of the study is to analyze the ISMS in 5 hospitals which contain more than 500 beds and to find out the level of personal health information security in compliance with international standards on information security such as ISO/IEC 27001; 17799, JIS Q 15001 in Japan and ISMS presented by Korean Internet & Security Agency in Korea. Also, the purpose is to recommend the standards on information security and security countermeasures which are fit for international standards and the needs of hospitals concerning information security, management, physical aspects, and technical aspects.

As analyzed, the conditions of the ISMS in 5 hospitals in Korea showed that the level of the ISMS in hospitals were rather low compared to the financial, manufacturing, and public institutions [8]. The lowest standards were found in the clauses of information asset management, information security incident management and continuity controls among the 11 clauses suggested by the ISMS. To establish security countermeasures, the following are required.

In terms of management, hospitals should review existing policies and be equiped with detailed policy documents including statements, regulations, guidance etc. in accordance with internal and external changes [9,10]. Also, it is required to organize an information security team with clear roles and responsibilities for security of information. Employment contract documents for new employees should contain the responsibilities of information protection, and hospitals should set up procedures for termination or changes of employment. As well as ensure education and evaluation schedules to train all staff. With the increase of outsourcing for business efficiency and cost-effectiveness in hospitals, security requirements should be suggested in third party agreements. For compliance, restrictions on IPR are reinforced strictly. Considering secure auditing, a new check list is required for internal and external security auditing.

In the physical and environmental aspects, secure areas should be defined and specified, and physical entry controls for the security of information assets are required. The disposal and re-use of equipment, removal of property, and security of equipment off-premises should be prescribed as well.

In technical aspects, new security vulnerability could be detected continuously through the development of information technology. So, hospitals should build up counter-plans at the starting point of medical information systems. Countermeasures for secure medical information systems should be established in accordance to information technology trends such as mobile codes. The leakage of personal information not only happens on-line through networks, but also through removable media including USB, CD-ROM, and magnetic tapes. Especially with the increase of the USB, a security measures for USB is desperately needed. For the future on-line exchange of medical information between hospitals, security policies and procedures for exchange of information should be set up immediately. Forgery, alternation and access of unauthorized staffs to log data on medical information systems should be protected at a reasonable cost. User password management is most important for maintaining effective access control and to ensure the security of the information systems. To avoid unauthorized access, a clear desk and screen or log-out should be implemented when staffs leave their office or computers. In cases of information system acquisition and development, it is considered a business requirement statement which describes in detail concerning information protection. Generally, it requires a lot of extra costs and effort to reflect security requirements when operating the system more than 60 times. With increasing hacking of technology, the scope and level of technical vulnerability needs to be determined and reviewed regularly. Though

doi: 10.4258/hir.2010.16.2.89

there are no compulsive regulations for disaster recovery systems in hospitals for security incident actions and business continuity, a security incident action system is required. Also it is important to follow-up security incidents as well as to prevent them. Disaster recovery systems cost very much, therefore a proper measurement is studied with in its scale.

It could be a big burden to hospitals in terms of cost and manpower for the improvement of insufficient clauses for information security to be verified. However it is necessary to establish the ISMS in hospitals in order to give trust to patients ensuring their privacy and to use medical records for various purposes in safety. The most important thing is the will to practice ISMS and try to meet the international standards for information security with long-term and comprehensive perspectives and review them regularly. Hospitals can approach information security from feasible security requirements such as policy and regulation making or supplementation of security faults. Also, it is necessary to reflect on the requirements of varied interests such as medical staff, medical consumers and other institutions for information security.

This study has limitations in that it analyzed ISMS for only 5 hospitals, so it could not represent the level of information security for all hospitals. However it is the first attempt to analyze the ISMS of the whole hospital including policies, organization, manpower, facilities and the information system. In addition, it suggests that the information security countermeasures based on international standards with reflecting the characteristics of hospitals. Suggested information security countermeasures could contribute to an improvement of information security in hospitals and may establish political support by setting up regulations and expenditure on ISMS in hospitals.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

References

1. Jung BJ. Present situation and problems of U-healthcare service (Ubiquitous Society Research Series 10) [Internet]. Seoul: National Information Security Agency; 2005 [cited at 2010 May 4]. Available from: http://old.nia.or.kr/open_content/board/boardView.jsp?id=28795&tn=CV_0000224.
2. Kim HE, Kim JH. A survey on the attitude of social groups toward security, privacy, and confidentiality of health information: an original paper authors and affiliations. J Korean Soc Med Inform 1999; 5: 63-76.
3. Kim ON. Registration of medical information and effective data collecting of information for survey and personal information protection methods, registration of medical data and information control for survey. In: Proceedings of Korea Medical Record Association Annual Fall Conference; 2003 September 26-27; Gyeongju. Seoul: Korea Medical Record Association; 2003. p32-35.
4. International Organization for Standardization. ISO/IEC 17799: Information technology--security techniques--code of practice for information security management. Geneva: International Organization for Standardization; 2005.
5. International Organization for Standardization. ISO/IEC 27001: Information technology--security techniques--information security management system-- requirements, international standard. Geneva: International Organization for Standardization; 2005.
6. Japanese Industrial Standards Committee. JIS Q 15001: Personal information protection management systems: requirements. Tokyo: Japanese Standards Association; 2006.
7. Korea Internet & Security Agency. ISMS certification inspection standards. Seoul: Korea Internet & Security Agency; 2008.
8. Center for Interoperable EHR. Report of development of information protection and security system. Seoul: Center for Interoperable EHR; 2009.
9. Korea Health Industry Development Institute. Guidance for hospital evaluation program. Seoul: Korea Health Industry Development Institute; 2007.
10. Lee EJ, Kim SY, Chae YM. Legislation direction for health information privacy in the telemedicine era. J Korean Soc Med Inform 2009; 15: 361-371.