ICIC Express Letters
Part B: Applications
Volume **11**, Number **7**, July **2020**

 ISSN 2185-2766
pp. 705–712

A STUDY ON SECURITY EVALUATION MODEL OF SMALL AND MEDIUM SIZE HEALTHCARE INSTITUTIONS

Jawon Kim[1] and Hangbae Chang[2]

[1]Department of Security Convergence
[2]Department of Industrial Security
College of Business and Economics
Chung-Ang University
47, Heukseok-ro, Dongjak-gu, Seoul 06974, Korea
{ jjawon; hbchang }@cau.ac.kr

Received January 2020; accepted April 2020

Abstract. *Recently, as a result of the 4th Industrial Revolution, the convergence service environment has changed and new security threats are emerging. Therefore, small and medium size healthcare institutions also require specialized security considering the business environment. Therefore, in this paper, the security characteristics of medical institutions were derived through analysis of previous research, and the characteristics and status of small and medium size healthcare institutions were surveyed through field surveys of small and medium size healthcare institutions. And also we design the security management evaluation model for small and medium size healthcare institutions based on the security characteristics of small and medium medical institutions. For the design, we compare and analyze existing security management system and evaluation certification system of medical institutions and verify the proposed security management evaluation model and degree of sharing. In addition, statistical verification of the designed security management evaluation model was performed. We expected to be able to build a valuation model considering security management characteristics of small and medium size healthcare institutions by the findings of this study.*

Keywords: Small and medium size healthcare institutions, Security characteristics, Security management system, Healthcare security

1. **Introduction.** The healthcare environment that records patients' healthcare information in the past has changed from the digital environment to the recording and management environment instead of paper due to the remarkable development of IT. This change in the healthcare environment has enabled users to receive services that enhance the convenience of patients' healthcare, such as telemedicine and wearable devices, and the paradigm of healthcare, which was centered on medical institutions, has changed to users. In the healthcare IT convergence environment, digitalized healthcare information includes the patient's personal information and is shared with various organizations including the insurance companies as well as the healthcare institutions through the network.

Therefore, leakage of healthcare information can lead to secondary damage through combination with patient's financial records, biometric information, and the like. In addition, since healthcare information includes sensitive information including personal health information and medical records, leakage of simple medical information can cause enormous damage. However, the level of security is still insufficient compared to the use of high IT technology in healthcare institutions and the importance of personal information. According to security experts, 99% of physicians have mobile devices and are actively using them to share patient information, but 14% of doctors use only one password.

DOI: 10.24507/icicelb.11.07.705

In addition, three major US hospitals have recently suffered extensive damage from Ransomware 'Locky' infections. It is time to investigate the security issues and threat trends facing us in order to prepare for the increasing number of healthcare security accidents, and to study the healthcare security issues from the technical and administrative level.

In order to confirm the actual cases of accidents at domestic and overseas healthcare institutions, the statistical analysis report of the Identity Theft Resource Center (ITRC), the research report of SANS Institute (SysAmin, Audit, Network and Security), and the research report of the Government Accountability Office (GAO) are studied. Through ITRC's recent statistical data, it was confirmed of the security threats. As shown, out of 614 cases of total data infringement, 269 cases were related to healthcare information, which is 43.8% of the total. Compared to the number of data threats in other industries, 23 data-intrusion accidents occurred in financial information, which indicates that hacker's interest in healthcare information is very high. In this way, security accidents in the healthcare field are frequently encountered and the damage is increased.

At the same time, the domestic and foreign countries are carrying out policies focusing on the information security management and evaluation of the healthcare institutions through the certification of the information protection management system such as ISO 27799 and K-ISMS. Especially, as a result of the amendment of the Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc., the Senior General Hospital under the Medical Service Act, which has annual sales of over KRW 150 billion, was subject to be certified the ISMS (Information Security Management System).

There are two main criteria for the classification of healthcare institutions in Korea, which are classified by the Medical Service Act and the National Health Insurance Act. According to the Medical Service Act [1], they are largely divided into clinic and hospital classes, and classified into general hospitals and advanced general hospitals according to certain standards of hospital healthcare institutions. According to the National Health Insurance Act [2], healthcare services are classified based on the healthcare delivery system and classified into primary, secondary, and tertiary healthcare institutions. The primary healthcare institutions are limited to healthcare institutions with less than 30 beds, including clinics and public health centers, that perform outpatient care. Secondary healthcare institutions are hospitals and general hospitals and are limited to healthcare institutions with more than 30 beds. The tertiary healthcare institutions are divided into higher general hospitals.

According to the data of the National Statistical Office [3], there are 43 tertiary hospitals, 301 general hospitals, 1,516 special hospitals, 1,462 hospitals and 30,689 clinics in accordance with the classification of healthcare institutions. This paper focused on small and medium size healthcare institutions such as hospitals and clinics which were located about 32,151 (94.53%). However, in case of the information protection management system implemented in Korea, it has only general information protection management system for general companies and it is implemented without consideration of the characteristics of healthcare institutions. Nevertheless, it is true that the introduction of the information protection management system of large healthcare institutions has a great influence on the improvement of the security level of domestic healthcare institutions.

However, small and medium size healthcare institutions have limitations in performing security activities due to their human and economic limitations compared with large healthcare institutions, and the security level of the organization members is so low that they do not feel the necessity of healthcare security sufficiently. It is urgent to take measures to improve the security level of small and medium size healthcare institutions which have relatively many institutions.

2. **Precedent Study on Security Characteristics of Healthcare Institutions.** Classification criteria were designed to derive the security characteristics of small and medium size healthcare institutions based on previous research. First, considering that security is the maintenance of the organization's well-being and order from the criminal activity performed by a person, healthcare security is checked the Player and the Type (Wilful, Mistake). In order to derive the security characteristics specific to the healthcare institutions based on the criteria, we analyzed the security incident scenarios occurring in the healthcare institutions through the previous research.

Based on the studies of Annex-A of ISO 27799 [4] and Nicole van Deursen [5], we derived frequent security characteristics from healthcare institutions.

Player is an insider, authorized third party, unauthorized third party, etc. The results were derived with the risk factors caused by wilful (abuse) and mistake (misuse) of each player.

As a result of analyzing previous studies, it was found that security incidents caused by insiders were the most common, and the frequency of occurrence of the scenarios was also the highest. The security incident scenarios related to the IT systems are in a very large amount. However, the actual occurrence frequency is confirmed, and five scenarios are security incidents that occur in actual medical institutions.

And we have checked when the frequency of occurrence is classified into five points, that scenario was allocated 1 (almost no) and 2 (none). Through this, it can be confirmed that the security accidents frequently occurring in the actual medical institutions are accidents caused by misuse or abuse by internal persons.

From the result of analysis of precedent studies, security management systems for healthcare institutions almost focused on large healthcare institutions. However, this paper proposed security management systems focused on small and medium size healthcare institutions. In case of small and medium size healthcare institutions they do not have enough money, time, and human resource. So, this paper proposed security management systems considerable for small and medium size healthcare institution's characteristics.

3. **Deriving the Security Characteristics of Small and Medium Size Healthcare Institutions.** In this paper, the security characteristics of small and medium size healthcare institutions are derived by reflecting the business characteristics of the healthcare institutions analyzed through the previous studies for small and medium size healthcare institutions.

Also in this study, detailed items of the security management evaluation model for small and medium size healthcare institutions were derived based on the previous research on the security characteristics of the healthcare institutions and on the status of the small and medium size healthcare institutions and the actual analysis contents.

We have compared the security checklist and the indexes for the healthcare institutions home and abroad including the detailed items and the existing general security management system (ISO 27001:2013 & 27002:2013 [6]) and ISO 27799:2016 [4].

This paper constructed a security management model that reflects the characteristics of small and medium size healthcare institutions and comparative analyses of previous studies including domestic and abroad standards related to healthcare security, and the list of previous studies analyzed in this study is shown in Table 1.

The analysis was done through the mapping based on the control items of each data or the details of the evaluation index. The mapping method is performed through the process of mapping similar or identical contents based on the lowest level of details held in each index. Through this step it is constructed a security management model that reflects the characteristics of small and medium healthcare institutions.

The operational definition of each sub-item derived from this study is shown in Table 2, and the definition was derived based on the previous research analyzed. The previous

TABLE 1. The list of certification related with small and medium size healthcare institutions

No.	Title
①	ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements, (2013)
②	Health Informatics – Information Security Management in Health Using ISO/IEC 27002, (2016)
③	An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, NIST Special Publication 800-66 Revision 1, (2008)
④	Joint Commission International Accreditation Standards for Hospitals, 5th Edition, (2014)
⑤	Japan Council for Quality Health Care, Hospital Accreditation Standards by Functional Category Hospital Type 1
⑥	Quality and Outcomes Framework Guidance for GMS Contract 2013/14, NHS Commissioning Board, (2013)
⑦	CQC, The State of Health Care and Adult Social Care in England: An Overview of Key Themes in Care 2010/11, Care Quality Commission, London, (2011)
⑧	de Sante, H. A. Haute autorite de Sante, Grossesses à risque: orientation des femmes enceintes entre les maternités en vue de l'accouchement, 2010-04, (2008)
⑨	The Australian Commission on Safety and Quality in Health Care, National Safety and Quality Health Service Standards (2nd Edition), (2017)
⑩	Joint Commission of Taiwan, Evolution of Hospital Accreditation Standards, (2015)
⑪	KISA, Information Security Management System (ISMS) Certification Standard, (2013)
⑫	Healthcare Institution Evaluation Guidelines, Ministry of Health and Welfare, Korea Health Industry Development Institute, (2017)
⑬	Security of Privacy Self-Checklist (Medical Institution), Korean Hospital Association, (2017)

researches referenced in the operational definition of the sub-items are described in the same order as in Table 1. This paper analyzes component of certification related small and medium size healthcare institutions. So, we derive 12 components which were based on same contents between each certification.

In addition, in selecting the sub-items, detailed items were selected to reflect the limitations of healthcare security and the current state of IT infrastructure in hospitals and hospitals currently operating system in Korea. In selecting and elaborating the detailed items, we focused on the limitation of current domestic hospitals and items with priority in international standard or certification system. The details of the proposed small and medium size healthcare institution security management evaluation model are shown in Table 2.

When we checked the details of each item and the degree of sharing the previous studies, the item "Healthcare institutions staff (General)" showed the highest score of 92%, followed by "Healthcare information security management" 85%, "Healthcare security staff", and "Continuous improvement (Certification)" 69%.

On the contrary, "Healthcare equipment (Specialized)" and "Compliance" showed the lowest degree of sharing with a 38% degree of sharing.

In order to improve the security level of small and medium size healthcare institutions and to prevent security accidents as well as the security status of the small and medium healthcare institutions analyzed in the foregoing, it is necessary to use the "Healthcare

Table 2. The list of evaluation items

Title	Contents	Ref.
Accident management	Refers to the management of response regulations for accidents that harm business continuity, such as system malfunctions and outflow accidents at medical institutions.	①, ②, ③, ⑨, ⑩, ⑪, ⑬
Continuous improvement (Certification)	Refers to activities that continuously improve the security environment of medical institutions.	①, ②, ③, ④, ⑤, ⑥, ⑧, ⑨, ⑩
Healthcare equipment (General)	Refers to the IT equipment commonly used by the organization of the healthcare institution. It also manages access rights (account management), environment update (Fetch, SW update), installation and operation of security SW for personal computer (PC), service server and database and the like.	①, ②, ③, ④, ⑤, ⑨, ⑩, ⑪
Healthcare equipment (Specialized)	Refers to security management such as access rights management (account management), environment update (Fetch, SW update) for devices specialized for medical activities such as CT, X-ray, and scale.	①, ②, ⑤, ⑪, ⑫
Healthcare information security management	Refers to the security management of application programs that contain medical information such as EMR, OCS, and PACS.	①, ②, ③, ④, ⑦, ⑧, ⑨, ⑩, ⑪, ⑫, ⑬
Classify and manage security areas (Equipment)	Refers to the operation of physical security systems such as access control, intrusion alarm, and detection of immigration to perform physical security activities in relation to protected areas.	①, ②, ③, ⑤, ⑦, ⑧, ⑪, ⑬
Security system operation	Refers to performing security management by identifying/distinguishing between the protected area (e.g., treatment room, and examination room) and protective equipment (healthcare equipment, etc.).	①, ②, ③, ④, ⑨, ⑪, ⑫, ⑬
Healthcare security investment (Facility)	The amount of security investment (ratio) to sales amount (or IT investment amount). The amount of security investment (ratio): refers to the cost to invest in staff (security) + security consulting + security system construction.	①, ②, ③, ④, ⑨, ⑪, ⑫, ⑬
Healthcare security investment (Education)	The amount of security investment (ratio) to sales amount (or IT investment amount). The amount of security investment (ratio): the cost of investing in security education.	①, ②, ③, ④, ⑤, ⑩, ⑪, ⑫, ⑬
Healthcare institutions staff (General)	Refers to security activities for employees (General) such as security pledge and security education.	①, ②, ③, ④, ⑤, ⑥, ⑦, ⑨, ⑩, ⑪, ⑫, ⑬
Healthcare security staff	The degree of security staff (or additional staff) in the healthcare institutions.	①, ②, ③, ④, ⑤, ⑦, ⑧, ⑪, ⑬
Compliance	The extent to which the organization's security regulations and activities are consistent with laws and regulations related to healthcare institutions (such as the Medical Law, the Health Care Act, the National Health Promotion Act, the medical device technique).	①, ②, ③, ④, ⑦

institutions staff (General)", i.e., medical staff working at the healthcare institutions. We can confirm that security activities targeting general employees including all employees should be given top priority.

4. **Statistical Verification.** In order to verify the security management evaluation model for small and medium size healthcare institutions, the final goal of this study, the subjects for the survey were selected. The survey was conducted for general employees of healthcare institutions who do not perform full-time or full-time medical security-related tasks, including healthcare institution staff, doctors, and nurse, for verifying the validity of evaluation model for security management of small and medium size healthcare institutions. The average value (standard validity) of each subitem was 3.5 or more, indicating that it is suitable for the security management evaluation model of small and medium size medical institutions. The results of survey for validity are shown in Figure 1.

Items	Average	Standard deviation
Accident management	3.82	0.61
Continuous improvement (Certification)	3.54	1.04
Healthcare equipment (General)	3.61	1.07
Healthcare equipment (Specialized)	3.86	0.89
Healthcare information security Management	3.86	0.97
Classify and manage security areas (Equipment)	3.93	1.09
Security system operation	4.04	0.92
Healthcare security investment (Facility)	3.86	1.15
Healthcare security investment (Education)	3.86	1.04
Healthcare institutions staff (general)	4.00	0.94
Healthcare security Staff	3.96	1.00
Compliance	3.54	1.29

FIGURE 1. The result of validity

The AHP analysis was conducted to calculate the weight of each item based on the 12 detailed items of the security management evaluation model of the small and medium size healthcare institutions. The subjects were selected to secure a high quality of the survey subjects. The AHP analysis to assess the relative priorities of each criterion was conducted by healthcare practitioners with more than 10 years of experience or by healthcare security personnel performing ICT outsourcing of healthcare institutions. AHP survey was conducted for 10 subjects, survey was conducted using the 10-point scale, and the consistency index was also calculated.

The results of AHP analysis are like Figure 2. The AHP analysis of this study, in order of relative importance, 21% for "Healthcare security investment (Education)", 18% for "Healthcare institution staff (General)", and 11% for "Classify and manage security areas (Equipment)" have relative priority. This is similar to the results of the previous research analysis that "the security activities by the insiders or workers related to the healthcare institutions should be added more than the security activities by the medical IT systems".

Items	Weighted	Priority
Accident management	2.1 → 2.0	12
Continuous improvement (Certification)	2.4 → 2.5	11
Healthcare equipment (General)	4.7 → 5.0	8
Healthcare equipment (Specialized)	6.4 → 6.5	7
Healthcare information security Management	6.8 → 7.0	6
Classify and manage security areas (Equipment)	11.2 → 11.0	3
Security system operation	9.0 → 9.0	4
Healthcare security investment (Facility)	5.3 → 5.0	8
Healthcare security investment (Education)	21.0 → 21.0	1
Healthcare institutions staff (general)	18.3 → 18.0	2
Healthcare security Staff	8.7 → 9.0	4
Compliance	4.2 → 4.0	10

FIGURE 2. Deriving priorities (weights) through AHP analysis

5. **Conclusions.** In this paper, the security characteristics of healthcare institutions were derived through analysis of previous research, and the security characteristics and status of small and medium size healthcare institutions were examined. The security management evaluation model for small and medium size healthcare institutions was designed and verified based on the security characteristics of small and medium size healthcare institutions. In order to design, the degree of sharing was verified by comparing and analyzing existing security management system and evaluation certification system related to healthcare institutions. Although there is no mandatory security certification and evaluation system for small and medium size medical institutions that have a relatively large number of sites, the results of this study show the business environment and constraints of small and medium size healthcare institutions. It is expected that the proposed model that reflects the condition will be able to suggest practical measures and action plans for healthcare institutions. The limitations of this study are that they did not carry out the case study to apply the designed model to the actual organization by securing the validity through statistical verification. The future work is case study to apply the designed model to the actual small and medium size healthcare institutions for securing the validity.

Acknowledgment. This paper was supported by Korea Institute for Advancement of Technology (KIAT) grant funded by the Korea Government (MOTIE) (P0008703, The Competency Development Program for Industry Specialist).

REFERENCES

[1] *Medical Service Act*, Available from: http://www.law.go.kr, Retrieved on 24th June 2019.
[2] *National Health Insurance Act*, Available from: http://www.law.go.kr, Retrieved on 24th June 2019.
[3] *National Health Insurance Statistical Yearbook*, National Health Insurance Service, Health Insurance Review & Assessment Service, 2018.
[4] *ISO 27799 Annex A Threats to Health Information Security*, ISO, 2016.
[5] N. van Deursen et al., Monitoring information security risks within healthcare, *Computer & Security*, 2013.

[6] ISO/IEC 27001:2013, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, ISO/IEC, 2013.
[7] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, NIST Special Publication 800-66 Revision 1, 2008.
[8] *Joint Commission International Accreditation Standards for Hospitals*, 5th Edition, Joint Commission Resources, Inc., 2014.
[9] Japan Council for Quality Healthcare, *Hospital Accreditation Standards by Functional Category Hospital Type 1*, 2014.
[10] *Quality and Outcomes Framework Guidance for GMS Contract 2013/14*, NHS Commissioning Board, 2013.
[11] CQC, *The State of Healthcare and Adult Social Care in England: An Overview of Key Themes in Care 2010/11*, Care Quality Commission, London, 2011.
[12] De Sante, H. A. Haute autorite de Sante, *Grossesses a risqué: orientation des femmes enceintes entre les maternites envue de l'accouchement*, 2010-04, 2008.
[13] *National Safety and Quality Health Service Standards*, 2nd Edition, The Australian Commission on Safety and Quality in Health Care, 2017.
[14] *Evolution of Hospital Accreditation Standards*, Joint Commission of Taiwan, 2015.
[15] *Information Security Management System (ISMS) Certification Standard*, Korea Internet and Security Association, 2013.
[16] *Healthcare Institution Evaluation Guidelines*, Ministry of Health and Welfare, Korea Health Industry Development Institute, 2017.
[17] *Security of Privacy Self-Checklist (Medical Institution)*, Korean Hospital Association, 2017.
[18] S. Biswas, J. H. Yoo and C. Y. Jung, A study on priorities of the components of big data information security service by AHP, *Journal of Society for e-Business Studies*, vol.18, no.4, 2013.