ICIC Express Letters
Part B: Applications
Volume **12**, Number **2**, February **2021**

ICIC International ©2021 ISSN 2185-2766
pp. **161–168**

DEVELOPMENT OF THE REVISED SECURITY MANAGEMENT MODEL FOR SMALL AND MEDIUM SIZE HEALTHCARE ORGANIZATIONS

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
84, Heukseok-ro, Dongjak-gu, Seoul 06974, Korea
{ jjawon; hbchang }@cau.ac.kr

Received August 2020; accepted October 2020

Abstract. *In the processing of patients' sensitive information, security attacker leaks the data. The healthcare data included not only medical record, but also sensitive information such as insurance information, social security number. For these reasons, healthcare information is frequently being a target of security attacks by outside attackers. In order to prevent security threats, healthcare organizations are adopting and operating a security management model. However, small and medium size healthcare organizations lack time and money, causing a difficulty in conducting security activities. Accordingly, our proposed security management model promotes performing security activities and suggests security priorities by deriving importance-level by each management control. Moreover, implementation is also provided in order to conduct suggested model, aiming at a higher practice in the field of small and medium size healthcare organizations.*
Keywords: Healthcare information life cycle, Security management model, Small and medium size healthcare organization, Analytic hierarchy process

1. **Introduction.** In the past healthcare organizations such as hospital, record on the paper the patient's data. Recently, due to remarkable development of information communication technology, they recorded and managed on the digital file. 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 healthcare organizations such as hospital, 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 organizations through the network.

Since sensitive information of patients is shared and used by various stakeholders, if the information leakage incidents occur, the scale of data is large. According to survey conducted by Health IT Security, the professional healthcare security press, it is said that healthcare information of patients of 974,000 has been leaked in University of Washington Medical Center in February 2019. This security incident occurred due to staff member's mistake, by changing a server setting which enabled a file search of patients' healthcare information from outer side. Due to this incident, patients were able to download healthcare information by searching their own name on search engine such as Google, and this online healthcare leakage lasted for about 3 weeks. Likewise, if healthcare information leaks, the healthcare organization goes to face on massive economic risks. It is time to investigate the security issues and threat trends facing us in order to prepare for the

DOI: 10.24507/icicelb.12.02.161

increasing number of healthcare security incidents, and to study the healthcare security issues from the technical and management level.

In order to respond to these security threats, healthcare organizations are conducting security activities. In case of Korea, laws are regulated to perform security management only at general hospital. According to ETNEWS [2], as a result of survey, targeted 150 of small and medium sized healthcare organization, showed that the ratio of security investment compared with investment of information system was only 7.58%. Also, the small and medium size healthcare organization which has security employee was only 2%. And the small and medium size healthcare organization who has the experience of security education was 27.3%. According to Korean Hospital Association [3], those healthcare organizations are in financial difficulties. So, scaled down healthcare organizations have limitations in performing security activities due to their human and economic limitations compared with large healthcare organizations, 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 organizations which have relatively many organizations.

In this research, we developed a healthcare security management model which was reflected of security characteristic in healthcare organizations. Also, we proposed security controls to secure small and medium size healthcare organization. This study improves the level of security in healthcare organizations and ultimately contributes to their business continuity.

2. Literature Review on Security Characteristics Healthcare Organizations.

2.1. Status of small and medium size healthcare organizations.

This study defined the healthcare organizations as medical institutions like hospital. In case of small and medium size healthcare organizations, they have small size IT system. IT system is mainly used in registration, payment, medical treatment PC, medical equipment for examination, data server and has a small number of types of devices. However, medical devices have different characteristics compared to general information communication devices. Medical devices are usually expensive equipment and have a characteristic of not being able to have periodical maintenance management due to cost problems after introduction and building medical devices to healthcare organization. Due to this problem, medical equipment and IT system mainly utilize legacy system. Moreover, due to a characteristic of not changing an once-established IT system, for example, utilizing Window XP, which is a terminated service from Microsoft, IT system in small and medium sized healthcare organizations is unable to update security patches in time, resulting in becoming vulnerable to diverse security threats.

In this research, a general IT system is established in doctors' office-level of hospital as shown in Figure 1. Figure 1 was changed in comparison with published paper [1]. This section is an additional research and analysis about status of small and medium sized healthcare organizations due to the fact taht the previous study missed it out. Figure 1 shows consideration for environmental characteristics of IT system in small and medium size healthcare organizations [4]. IT is largely shown as PC, medical equipment, server devices and patient information which includes medical record, prescription information, accounting information, PACS information, etc. are the information used in one-time medical treatment. Data server is described in Figure 1. However, small size of doctors' office-level hospitals does not have server and instead, has a network constructed which enables transmitting and receiving between each PC device. Like so, small and medium size healthcare organizations are classified as hospital, which handle diverse sensitive information, but still have vulnerable environment to security threats since basic security

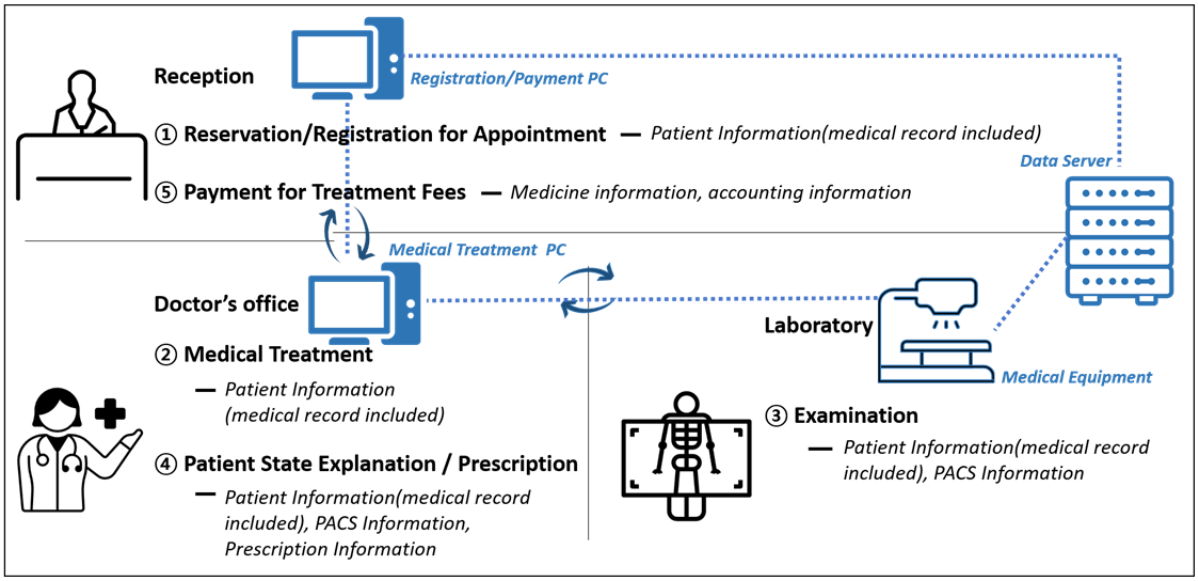

FIGURE 1. Status of small and medium size healthcare organization environment

activities such as data access control, separation of network, and usage of up-to-date security software, are not properly conducted.

2.2. **Characteristics of small and medium size healthcare organizations.** To design the security management model for small and medium size healthcare organization, this study analyzed security characteristics of scaled down healthcare organization. The classification criteria were designed to derive the security characteristics of small and medium healthcare organizations based on previous research. First, considering that security is the maintenance of the organization's business continuous and order from the criminal activity performed by a person, healthcare security is checked the Player and the Type (Willful, Mistake). In order to derive the security characteristics specific to the healthcare organizations based on the criteria, we analyzed the security incident scenarios occurring in the healthcare organizations through the previous research.

Based on the studies of Annex-A of ISO 27799 [5] and Nicole et al. [6], we derived frequent security characteristics from healthcare organizations. Player is an insider, authorized third party, unauthorized third party, etc. The results were divided with the risk factors caused by willful (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 occurrence frequency of the scenarios was also highest. The security incident scenarios related to the IT systems are very large amount. However, the occurrence frequency is checked, and five scenarios are security incidents that occur in actual medical organizations.

The form of security incidents in healthcare organizations differs by the life cycle of healthcare information. Healthcare information is generated and collected and then stored in internal system when patient intends to get treatment. Stored healthcare information conducts treatment and examination, gets updated and shares information with government agency such as Ministry of Health and Welfare, and Health Insurance Review & Assessment Service. Security attacks that can occur throughout the generation and destruction of healthcare information can be structured as Table 1 below. Table 1 was changed in comparison with published paper [1]. This part is an additional research about the security incidents which could happen based on the healthcare information life cycle which was the information collection to destruction.

TABLE 1. Security incidents by healthcare information life cycle

Healthcare information life cycle	Offender	Security incidents
Generation/Collection	– Insider	– Omission on agreement for particular section regarding provision and utilization of healthcare information on purpose in the perspective of information management. – Utilization of patients collected private information for anything other than original intend in the perspective of information management.
Storage/Process	– Insider – Authorized third party (IT outsourcing)	– Omission on encryption regarding important information. – Omission on log record regarding user accessed to database (arbitrary elimination).
Provision/Utilization	– Insider	– Illegal provision of healthcare information toward external institution (corporation) or individual beyond the range of healthcare information security.
	– Authorized third party (IT outsourcing)	– Availability of leakage by external employee (authorized third party) in charge of maintenance of healthcare information system (website, etc.) which includes patient (private) information.
	– Insider – Authorized third party (IT outsourcing)	– Grant excessive access authorization on healthcare information for each employee/department.
Destruction/Disuse	– Insider	– Healthcare organizations (hospital) who collected healthcare information and external institutions who was provided with healthcare information storing healthcare information without destruction regardless of the requirement for destructing healthcare information after utilizing for business handling.

The types of user who can induce corresponding security incidents are classified [7]. User referred in Table 1 mainly consists of insider (hospital employee), authorized third party (IT system outsourcing administrator, maintenance administrator, etc.). Moreover, it is also necessary to consider the risk of always being exposed on outsider (hacker) throughout the entire process of usage of hospital's internal IT system. Healthcare information contains sensitive information including private information. In case of information leakage to the outside, it has a characteristic of secondary damage through Personal Identification Number. These are illegal transaction at higher rate compared to other information, resulting in high possibility of leakage incidents by various users.

3. Proposed Security Management Model for Small and Medium Size Healthcare Organizations.

In this paper, the security characteristics of small and medium size healthcare organizations are derived by reflecting the business characteristics. Also, the proposed detailed controls of the security management model were derived based on the previous research on the security characteristics of the healthcare organizations and on the status of the small and medium size healthcare organizations.

The analysis was done through the mapping based on the controls of each data or the details of the management 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 construct a security management model that reflects the characteristics of small and medium healthcare organizations. The operational definition of each sub-control derived is shown in Table 2 below, and the definition was derived based on the previous research analyzed. Table 2 was changed in comparison with published paper [1]. This study added the reference for designing the security management controls

Table 2. The list of security management controls

Title	Contents	Ref.
Healthcare security related law (compliance)	Refers to a law related to healthcare security which includes healthcare, private information, information and communications network related law	[9,14,15]
Healthcare security organization	Refers to a degree of organization and security staff (or additional staff) members in healthcare organizations	[5,8,9,11,12,16]
Healthcare security consciousness	Refers to the amount of security investment (ratio) to sales amount (or IT investment amount): the cost of investing in raising awareness, education, security investment, security consulting, etc.	[5,8-12,16]
Healthcare security system	Refers to the security management of security management, physical security systems operation, IT equipment, application programs which contain healthcare information (EMR, OCS, etc.), access rights, environment update (Patch, SW update)	[5,8,9,11-13]
Healthcare security regulation	Refers to the organization's security regulation which is established and regularly improved the contents, furthermore they also refer to publishing the regulation	[5,8,9]
Healthcare security certification	Refers to activities that continuously improve the security environment healthcare organizations	[5,8-10]
Healthcare security incident response	Refers to a management of incident response that harms business continuity, such as system malfunctions and leakage in healthcare organizations	[5,8-11]

compared with previous study [1]. As a result, the number of control and its meanings are changed. This paper analyzes component of certification related small and medium size healthcare organizations. So, we derived 7 components which were based on the same contents between each certification.

When we checked the details of each control and the degree of sharing the previous studies, the control "Healthcare Security Consciousness" showed the highest score of 70%. On the contrary, "Healthcare Security related Law (Compliance)" and "Healthcare Security Regulation" showed the lowest degree of sharing with a 30% degree of sharing. These regulations are established in order to improve the security level of small and medium size healthcare organizations. And the regulations are designed to prevent security incidents as well as the security status of the small and medium healthcare organizations analyzed.

4. **The Design and Verification in Security Management Model.** In order to verify the security management model for small and medium size healthcare organizations, the subjects for the survey were selected. The survey was conducted for general employees of healthcare organizations who do not perform full-time or medical security-related tasks, including healthcare organization staff, doctors, nurse. The importance such as standard validity of each sub-control was 3.5 or more, indicating that it is suitable for the security management model of small and medium size medical organizations. The results of survey for validity are as below in Table 3. Table 3 was changed in comparison with published paper [1]. We verified the importance and weights of newly designed controls. Also, the survey was the questionnaires that the proposed security management controls were suitable or not for small and medium size healthcare organization. Through analytic hierarchy process, we verified the control's weight of both general healthcare organization and small and medium size healthcare organization. The importance was verified by a five-point Likert scale and as a result, out of 7 detailed management controls.

As a result, "Healthcare Security Certification" was excluded, indicating the other 6 being verified as the security management control with the value equal to or over 3.5. Control "Healthcare Security Certification" was dismissed with the value of 3.34, resulting in

TABLE 3. The importance and weight of small and medium size healthcare compared with general healthcare organization

Control	Importance (maximum 5)	Weight of small and medium size healthcare organization (ratio, total 1)	Weight of general healthcare organization (ratio, total 1)
Healthcare security related law (compliance)	4.50	0.34	0.31
Healthcare security organization	3.50	0.10	0.18
Healthcare security consciousness	3.85	0.24	0.17
Healthcare security system	3.93	0.16	0.11
Healthcare security regulation	3.91	0.12	0.13
Healthcare security certification	3.34	0	0.5
Healthcare security incident response	3.94	0.4	0.5

inappropriate for small and medium size healthcare organizations. Subsequently, relative weights of management controls were drawn to conduct security management with consideration of priorities in small and medium size healthcare organizations. AHP analysis method is used to derive relative weights and calculate the weight of each control based on the 7 detailed controls of the security management model of the small and medium size healthcare organizations. The subjects were selected to secure a high quality of the survey subjects. The AHP analysis was conducted by healthcare practitioners with more than 10 years of experience or by healthcare security personnel performing ICT outsourcing of healthcare organizations. 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 shown in Table 3. Both relative weights for scaled down healthcare organizations and general healthcare organizations are drawn and the control "Healthcare Security Certification" was excluded, which was unverified for validity of security management control. In case of small and medium size healthcare organization, the most important control was "Healthcare Security related Law (compliance)" with taking up 0.34 for weights. When compared to general hospital, control "Healthcare Security Organization" was the most distinguished control, which had 0.8 points of higher importance for general hospital. In small and medium size healthcare organizations where security organization is relatively less important, realistic limitation of acquiring security experts exists, showing aligned result with the characteristic of holding an additional position as well as security related works.

This paper established security management model by taking the characteristics of small and medium size healthcare organizations into account with a minimal condition of requirements. However, difficulties of manpower and cost lie with small and medium healthcare organizations. Also, employees in small and medium size healthcare organizations have relatively low security awareness, making it difficult for them to recognize which security activities should be conducted to meet the management standard designed in this research. Moreover, this paper contributes in easy adaptation to small and medium size healthcare organizations with the suggestion of security implementation which can easily comply with management standard by considering the security characteristics of small and medium size healthcare organizations.

In order to conform with final 6 security management controls, total of 20 detailed implementations are composed. The implementations were reorganized that were referenced when designing the model and minimum of contents which must be conducted in small and medium size healthcare organizations was extracted to compose the implementations. The main contents are compliance method of management controls, preparation of necessary evidence materials for management of a legal and regulation basis for corresponding management model, etc. Management model, detailed controls suggested in this research

and the correlation between implementations are described in Figure 2 below. This Figure 2 was changed in comparison with published paper [1]. Although it is not mentioned in previous study, the implementation was composed to contribute to small and medium sized healthcare organization which have difficulty performing security countermeasures.

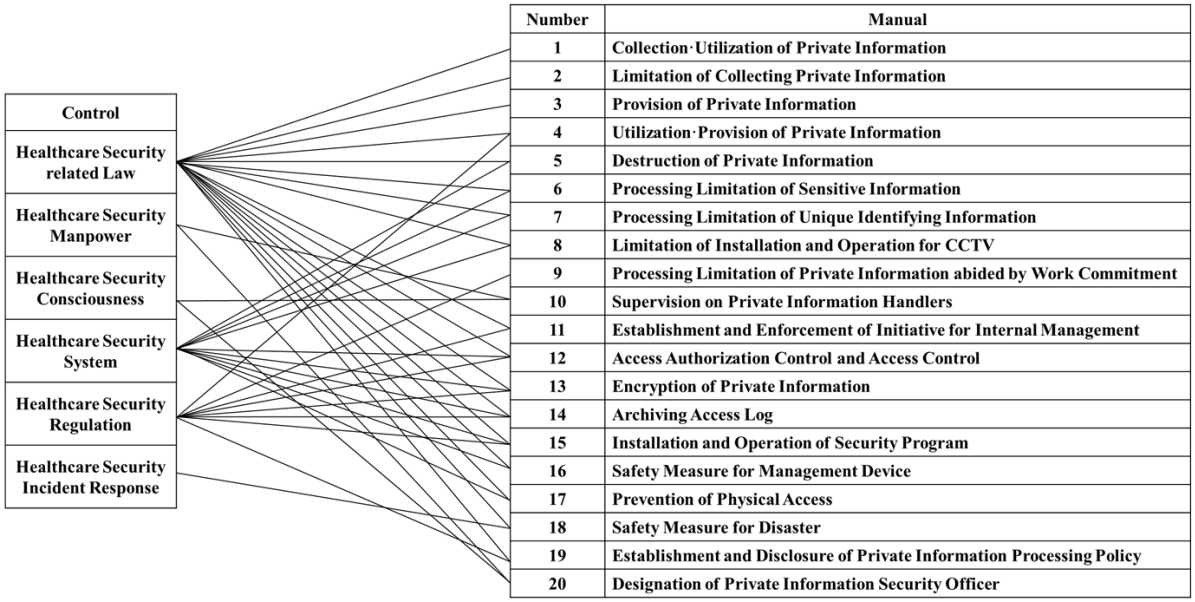

FIGURE 2. Implementation for security management model

5. **Conclusions.** This paper is a corrected version of "A Study on Security Evaluation Model of Small and Medium Size Healthcare Institutions" [1] in the errors of contents and acknowledgement. In detail, the first and second paragraphs in introduction, the preceding research, which summarized the environment and security threats of small and medium size healthcare organizations were changed. Also, the model derivation process was changed like as Table 3. So far, the number of proposed controls also has changed. In addition, AHP analysis method was applied to newly, and provided implementation which was applicable to the small and medium size healthcare organizations. Again, we apologize for confused about research paper to reader.

The proposed security management model for small and medium size healthcare organizations was designed and verified based on the security characteristics of small and medium size healthcare organizations. The security characteristics of healthcare organizations were derived through analysis of previous research. In order to design, the degree of sharing was verified by comparing and analyzing existing security management system certification system related to healthcare organizations. Also, implementation regarding management control is provided in order for small and medium size healthcare organizations to understand and perform suggested management controls with ease, aiming to contribute in high utility of application in the field. The limitations of this study are that they did not carry out the case study to apply the designed model to the 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 organizations for securing the validity. Moreover, the researchers should consider about security module which has the automated immunity [17]. The immune function is useful to the small and medium sized healthcare organization which lacks the human and system resource.

REFERENCES

[1] J. Kim and H. Chang, A study on security evaluation model of small and medium size healthcare institutions, *ICIC Express Letters, Part B: Applications*, vol.11, no.7, pp.705-712, 2020.

[2] Y. C. Jung, Re-challenge in the medical cloud market in 7 years, it can be suitable for both precision medicine and healthcare security, *ETNEWS*, https://www.etnews.com/20170208000130, Accessed on August 5, 2020.
[3] Korea Hospital Association, *The Current Issue of Hospital Information Security*, http://www.khanews.com/news/articleView.html?idxno=140766, Accessed on August 5, 2020.
[4] *Cyber Security Guide for Smart Medical Service*, Internet of Trust Security Alliance, 2018.
[5] ISO, 27799 health informatics security management in health using ISO/IEC 27002, *ISO*, 2016.
[6] D. Nicole et al., Monitoring information security risks within healthcare, *Computer & Security*, 2013.
[7] LG CNS Security Consulting Team, Your healthcare information does it safe?, *LGCNS Blog*, https://blog.lgcns.com/779, Accessed on July 29, 2020.
[8] ISO/IEC 27001:2013, Information technology security techniques information security management systems require-ments, *ISO/IEC*, 2013.
[9] An introductory resource guide for implementing the health insurance portability and accountability act security rule, *NIST Special Publication 800-66 Revision 1*, 2008.
[10] *National Safety and Quality Health Service Standards (2nd Edition)*, The Australian Commission on Safety and Quality in Health Care, 2017.
[11] *Information Security Management System Certification Standard*, Korea Internet and Security Association, 2013.
[12] *Healthcare Institution Evaluation Guidelines*, Ministry of Health and Welfare, Korea Health Industry Development Institute, 2017.
[13] C. G. Yang et al., A study on the antecedents of healthcare information protection intention, *Information Systems Frontiers*, vol.18, no.2, pp.253-263, 2016.
[14] United State of America, *The Privacy Act of 1974 (2020 Edition)*, 2020.
[15] Y. H. Bang, H. S. Rhee and I. H. Lee, A comparative study of regional medical information protection act and privacy act, *The Journal of the Korea Contents Association*, vol.14, no.11, pp.164-174, 2014.
[16] D. H. Yun, A study on knowledge, recognition, and practice of protecting the medical information in medium-small size hospital employees, *The Journal of Humanities and Social Science*, vol.10, no.5, pp.1439-1452, 2019.
[17] T. Okamoto, An immunity-enhancing security module for cloud servers, *International Journal of Innovative Computing, Information and Control*, vol.16, no.1, pp.137-151, 2020.