

Trends in Research on the Security of Medical Information in Korea: Focused on Information Privacy Security in Hospitals

Yong-Woon Kim, BA, MBA¹, Namin Cho, BS², Hye-Jung Jang, PhD³

¹Department of Management and Support, Yonsei University Dental Hospital, Seoul, Korea; ²Department of Medical Information and Communication Information Security, Yonsei University Health System, Seoul, Korea; ³Department of Clinical Trials for Medical Devices, Yonsei University Health System, Severance Hospital, Seoul, Korea

Objectives: Information technology involves a risk of privacy violation in providing easy access to confidential information, such as personal information and medical information through the Internet. In this study, we investigated medical information security to gain a better understanding of trends in research related to medical information security. **Methods:** We researched papers published on ‘의료정보’ and ‘medical information’ in various Korean journals during a 10-year period from 2005 to 2015. We also analyzed these journal papers for each fiscal year; these papers were categorized into the areas of literature research and empirical research, and were further subdivided according to themes and subjects. **Results:** It was confirmed that 48 papers were submitted to 35 academic journals. There were 33 (68.8%) literature review articles, and analysis of secondary data was not carried out at all. In terms of empirical research, 8 (16.7%) surveys and 7 (14.6%) program developments were studied. As a result of analyzing these papers according to the research theme by research method, 17 (35.4%) papers on laws, systems, and policies were the most numerous. It was found that among the literature research papers on medical personnel were the most common, and among the empirical research papers, research on experts in information protection and medical personnel were the most common. **Conclusions:** We suggest that further research should be done in terms of social perception, human resource development, and technology development to improve risk management in medical information systems.

Keywords: Electronic Health Records, Hospital Information Systems, Medical Informatics, Computer Security

Submitted: August 31, 2017

Revised: November 7, 2017

Accepted: December 22, 2017

Corresponding Author

Hye-Jung Jang, PhD

Department of Clinical Trials for Medical Devices, Yonsei University Health System, Severance Hospital, 50 Yonsei-ro, Seodaemun-gu, Seoul 03722, Korea. Tel: +82-2-2228-5150, E-mail: jhj0519@yuhs.ac

This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/4.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

© 2018 The Korean Society of Medical Informatics

I. Introduction

Modern daily life offers many conveniences due to the incredible speed of information and communication technology (ICT) and the Internet of Things (IoT), especially the ease of communication and access of information through the Internet and social network service (SNS). However, personal information can be leaked to the Internet and SNSs. To protect personal information, the Treaty of Personal Information Protection of the European Council (Treaty of the European Parliament for the Protection of Individuals Related to the Automatic Processing of Personal Informa-

tion) was established in 1980 [1]. In the same year, the Organization for Economic Co-operation and Development (OECD) provided the Guideline on Privacy Protection and Cross-Country Distribution of Personal Information [2]. A guide for the handling of personal information files was codified by the United Nations and was published in 1990 [3]. Rules for the handling, processing, and transmission of personal information in the European Union (EU) were then published in 1995 as the International Standard for the Protection of Individuals [4]. Medical information, the most important and sensitive personal information, should be particularly protected [5].

Although medical information should be protected in the Internet space, personal records created by medical institutions and medical treatment prescription computer networks can be infiltrated, resulting in spamming by commercial advertisements and product promotions. Thus, personal information is frequently misused. This problem must be addressed by laws and improvement of security of institutional equipment and systems used to handle personal information [6]. Nowadays, anyone can search for any information. Advances in technology provide us with ways to easily exchange personal information; however, this leads to the danger of infringement [7]. Medical information, as important and sensitive personal information, should be protected. Regarding information related to the provision of healthcare by national and local public health institutions, the information is generally gathered by doctors who directly provide medical care and services to patients. This means that materials are collected throughout the entire process, including diagnosis and the subsequent course of treatment, including information analyzed based on these materials [8]. Currently, medical information in the clinical environment of a hospital is conveniently managed by utilizing Electronic Health Record (EHR) systems without the need for paper records. However, criminal activities are actively being carried out to acquire personal information to perform illegal financial or monetary transactions. It is impossible to sufficiently protect personal medical information if there is no standard for medical information protection. We should not only take countermeasures against damages cause by medical information leakage; we must also take measures to prevent information leakage [9]. Medical information systems are intended store and share information among healthcare providers and to improve work efficiency of various hospital departments, prevent medical accidents, reduce the waiting time of patients, and prevent over-prescription or lack of prescription without requiring paper or film storage. It has

been demonstrated that such systems can reduce costs [10]. As a ubiquitous technology to enable the use of services anywhere any time, u-health (ubiquitous health) allows patients to receive medical services at places other than hospitals by sharing treatment paradigms among medical service providers and hospitals that respond to the illness; thus, healthcare services will be given in a more timely manner in the future.

However, we must always consider the security of shared systems that collect, store, and transfer medical information. Medical information includes extremely personal health information as well as information about a patient's lifestyle habits and physical features. The importance of storing such sensitive information has been emphasized to prevent personal information security problems, such as information leakage, hacking, tampering, and so on [11]. There have been no studies on trends in the security of medical information in Korea. This study was conducted to investigate trends in medical information security for personal information protection in Korea during the period 2005 to 2015 and to determine whether personal information is being protected properly.

II. Methods

1. Research Contents

In this study, we found that research on medical information was mainly focused on risk management of medical information systems at hospital-centered medical institutions rather than general agencies. We analyzed the contents of papers published in this area by theme, year, and research method. Our main objective was to produce results that would be useful for future research. Therefore, our research had the following aims: (1) to analyze medical information security-related papers based on theme and year and (2) to compare medical information security-related papers and analyze the research methods used.

2. Scope of Research Papers

The purpose of this research was to analyze the trends in research on the theme of medical information. Therefore, papers on medical information published in various domestic Korean journals from 2005 to 2015 were searched. On July 16, 2016, using academic research information service (RISS), a search site for published papers, 274 papers were obtained using the keywords of '의료정보' (medical information in Korean) and 'medical information'. Their information was extracted. On July 21, 2016, three experts reviewed these papers, and 74 papers were selected after this review.

The list of studies was chosen by sorting out the last 48 of 60 articles (Figure 1).

3. Medical Information Papers and Analysis Criteria by Year

In this study, we analyzed research papers related to medical information published from 2005 to 2015 to reveal the trends in current research approaches to guide the direction of future research. Based on 274 studies published, the research trends were classified. The results are shown in Table 1.

Considering recent research references after analyzing the research trends of papers on medical information, the papers were divided into categories of literature research and

empirical research. We prepared an analysis framework to facilitate our analysis.

More specifically, the field of medical information research cannot advance by only focusing on the sensitivity of the medical information of patients. Therefore, the papers were further classified into more specific research areas of computer systems, electronic medical records, and personal information protection.

III. Results

To observe the trends in research investigating medical in-

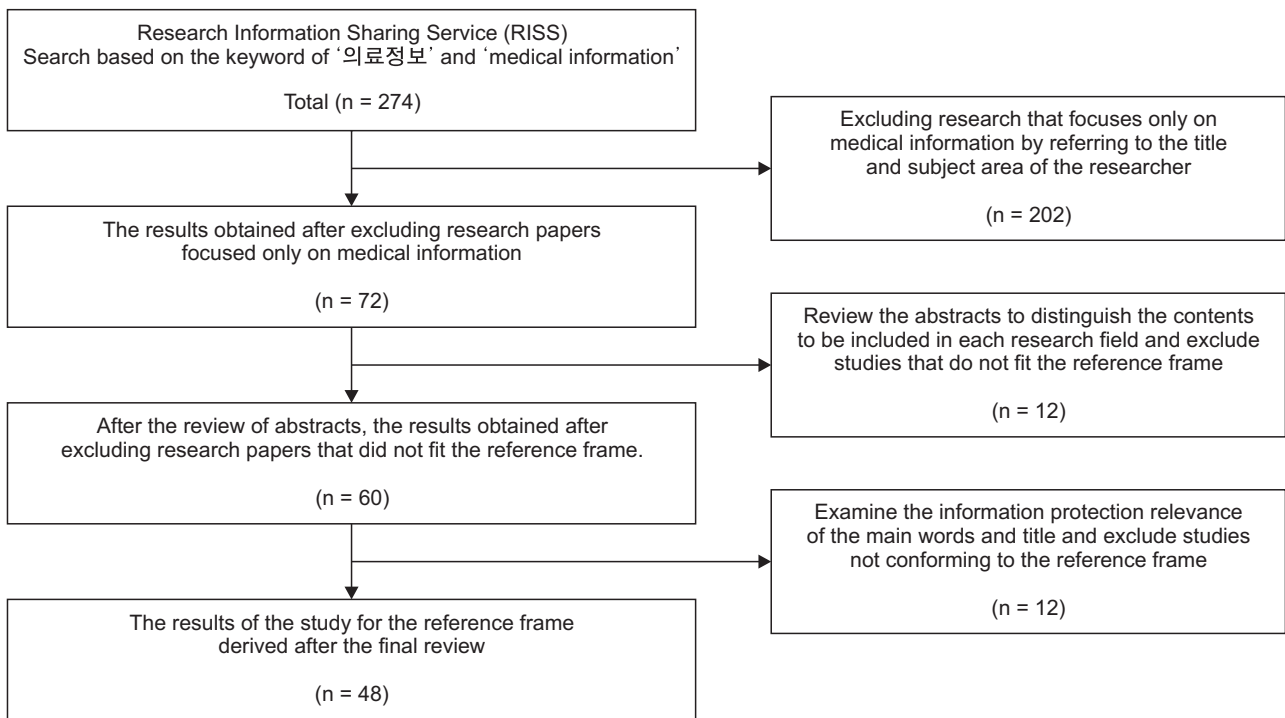


Figure 1. QUOROM flowchart for literature review about risk management of medical information system in Korea.

Table 1. Article classification process

Classification process	Method	Standard	Number of papers
Search for articles	Academic research information service (RISS)	Search keywords about medical information and medical information	274
1st classification	For the entire paper, the researchers are classified into individual classifications	Considering the title preferentially, do not refer to researchers' specialty fields	72
2nd classification	Three researchers joint confirmation	Based on the primary classification data, classify the contents included in each research field (abstract review)	60
3rd classification	Three researchers joint confirmation	Analysis after finally checking what is relevant to the relevant box (related to information protection of major word and title)	48

formation security, we categorized the papers by methodology into literature research and empirical research categories. The results are as shown in Table 2.

Literature research was found to have the highest number of published papers. There were 33 (68.8%) literature review papers published during the study period. The methodological approach adopted in empirical studies was to recruit groups and developed research and programs concurrently. Compared to the empirical study method, 8 (16.6%) survey research papers of 48 total papers were published, while 7 (14.6%) papers on methods of research in the practical field were published.

Detailed results are shown in Figure 2. Thirty-three (68.8%) theoretical papers were published among the total papers on

Table 2. Number of published articles by research method

Classification	Number of articles (%)
Literature research	
Theory	
Literature review	33 (68.8)
Secondary document analysis	0 (0.0)
Empirical research	
Experience	
Survey research	8 (16.6)
Deep interview	0 (0.0)
Focus group interview	0 (0.0)
Investigation + experiment	0 (0.0)
Practice	
Program development	7 (14.6)
Total	48 (100)

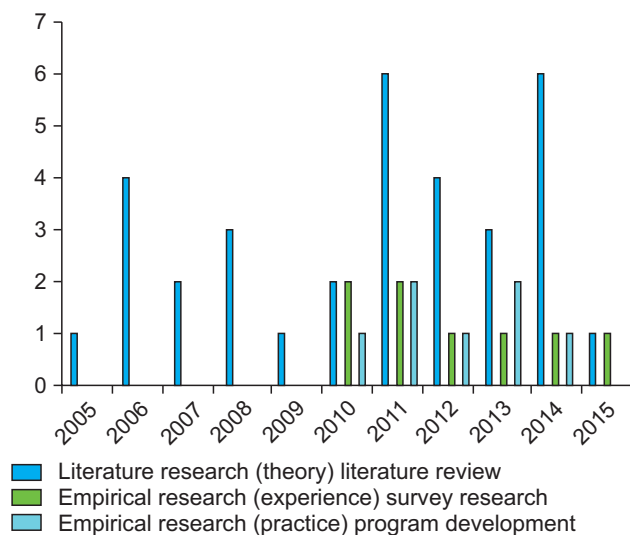


Figure 2. Number of articles published by period.

research methods. There were many literature review papers published that focused on analyzing methods. Literature reviews were carried out periodically. Analysis of secondary data was not performed at all. The field of empirical research was divided into survey research, in-depth interviews, focus group interviews, and investigations and experiments in parallel. Survey research was dominant every year. However, there were not in-depth interviews conducted during 2005–2015 each time period. There were no reports of focus group interviews or investigation and experiments in parallel either since 2005. There were 7 (14.6%) practice research papers among total research methods.

Results of our analysis on research on the management of medical information systems according to research methods and topics are shown in Figure 3. There were 17 (35.4%) papers published on laws, systems, and policies. There were no papers published on the topics of recognition of and satisfaction with medical information security. On the topics of actual situations, review discussions, trends, and factors, there were 5 (10.4%), 9 (18.8%), and 3 (6.3%) papers published, respectively. There were no papers on the topics of the effect and influence of medical information security. For measure topic, there were 2 (4.2%) papers published. On the topics of applications (program), utilization, and model development, 9 (18.8%), 2 (4.2%), and 1 (2.1%) paper(s) were published, respectively.

According to the method of research, there were 33 (68.8%) papers on literature studies and 15 (31.3%) papers published on laws, systems, and policies. There was no paper published on recognition and satisfaction. Actual situation topic had

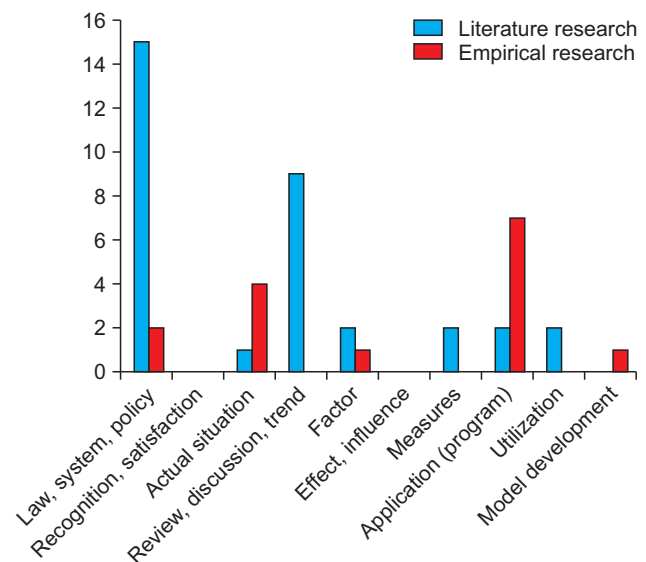


Figure 3. Number of papers by research theme and research method.

1 (2.1%) paper. Review discussion and trend topic had 9 (18.8%) papers while factor topic had 2 (4.2%) papers. However, there was no paper published on effect and influence. Topics of measures, applications (program), and utilization each had 2 (4.2%) papers published. However, there was no paper published on model development. The total number of empirical research paper was 15 (31.3%). Two papers (4.2%) were published on the topics of laws, systems, and policies. No papers were published on recognition and satisfaction. Four papers (8.3%) were published on the topic of actual situations. One paper (2.1%) was published on the topic of factors. No papers were published on review discussion, and trend, effect, influence, or measure topics. Application (program) topic had 7 (14.6%) papers while model development topic had 1 (2.1%) paper. However, utilization topic had no paper.

The results of our analysis of research on the management of medical information systems according to research methods and subjects are shown in Table 3. A total of 16 (8.7%) papers were studies on patients, while 101 (55.2%) papers were studies on medical-related workers. There were 46 (25.1%) papers on information-related experts, 1 (0.6%) paper on small and medium business centers (public institutions), 4 (2.2%) papers on healthcare agencies (hospital), 12 (6.6%) papers on government agencies, 2 (1.1%) papers on integrated medical information systems, and 1 (0.6%) paper on multidisciplinary approaches.

The results are as shown in Table 3. In more details, regarding medical-related workers, there were 18 (9.8%) papers on doctors, 17 (9.2%) papers on nurses, 2 (1.0%) papers on physical therapists, 15 (8.2%) papers on radiological technologists, 1 (0.6%) paper on students in the department of dental hygiene, 15 (8.2%) papers on pharmacists, 15 (8.2%) papers on clinical pathologists, 16 (8.7%) papers on medical record system managers, 1 (0.6%) paper on hospital administrative managers, and 1 (0.6%) paper on occupational therapists. Regarding information-related experts, there were 16 (8.7%) papers on security officers, 1 (0.6%) paper on expert computer officers, 17 (9.3%) papers on information handlers, 4 (2.2%) papers on information protection experts, and 8 (4.3%) papers on medical information experts. There was 1 (0.6%) paper on healthcare managers for small and medium business centers (public institutions). Regarding healthcare agencies (hospitals), there were 2 (1.0%) papers on hospital staff members; 1 (0.6%) paper on telemedicine users; and 1 (0.6%) paper on individuals, organizations, businesses, and organizations that handle health information. Regarding government agencies, there were 6 (3.3%)

papers on law, 1 (0.6%) paper on policy (Ministry of Health and Welfare), 1 (0.6%) paper on various international norms on the protection and utilization of personal information (OECD, EU), 1 (0.6%) paper on personal health information, 3 (1.6%) papers on privacy information security and medical privacy information security. There were 2 (1.0%) papers on integrated medical information system and 1 (0.6%) paper on multidisciplinary approach.

Based on research methodology, 165 (90.2%) studies were conducted as literature research, including 17 (9.3%) papers on doctors; 16 (8.7%) papers on nurses, persons in charge of medical record, security officers, and information handlers; 15 (8.2%) papers on radiological technologists, pharmacist, and clinical pathologist; 8 (4.3%) papers on medical information experts; 6 (3.3%) papers on laws; 2 (1.1%) papers on privacy information security and medical privacy information security; and 1 (0.6%) paper each for hospital administrative managers; occupational therapists; expert computer officers; individuals, organizations, businesses, and organizations that handle health information; policy (Ministry of Health and Welfare); various international norms on the protection and utilization of personal information (OECD, EU); and personal health information. There were no papers on physical therapists, students in the department of dental hygiene, information protection experts, healthcare managers, telemedicine users, hospital staff members, integrated medical information systems, or multidisciplinary approaches.

A total of 18 (9.8%) empirical studies were reported, including 4 (2.2%) papers on information protection experts; 2 (1.0%) papers each on physical therapists, hospital staff members, and integrated medical information systems; 1 (0.6%) paper each on doctors, nurses, students in the department of dental hygiene, information handlers, healthcare managers, telemedicine users, privacy information security and medical privacy information security, and multidisciplinary approaches. There were no papers on patients; radiological technologists; pharmacists; clinical pathologists; person in charge of medical records; hospital administrative managers; occupational therapists; expert computer officers; security officers; medical information experts; individuals, organizations, businesses, and organizations that handle health information policy (Ministry of Health and Welfare); various international norms on the protection and utilization of personal information (OECD, EU); personal health information; or law.

Table 3. Lists the research subjects and research papers by research method

	Literature research	Empirical research	Total
Patient	16	-	16 (8.7)
Medical-related person			
Doctor	17	1	18 (9.8)
Nurse	16	1	17 (9.2)
Physical therapist	-	2	2 (1.0)
Radiological technologist	15	-	15 (8.2)
Student in the department of dental hygiene	-	1	1 (0.6)
Pharmacist	15	-	15 (8.2)
Clinical pathologist	15	-	15 (8.2)
A person of medical record	16	-	16 (8.7)
Hospital administrative manager	1	-	1 (0.6)
Occupational therapist	1	-	1 (0.6)
Information-relates expert			
Expert computer officer	1	-	1 (0.6)
Security officer	16	-	16 (8.7)
Information handler	16	1	17 (9.3)
Information protection expert	-	4	4 (2.2)
Medical information experts	8	-	8 (4.3)
Small & medium business center (public institutions)			
Health care manager	-	1	1 (0.6)
Healthcare agency (hospital)			
Telemedicine user	-	1	1 (0.6)
Hospital staff	-	2	2 (1.0)
Individuals, organizations, businesses, organizations that handle health information	1	-	1 (0.6)
Government agency			
Policy (Ministry of Health and Welfare)	1	-	1 (0.6)
Various international norms on the protection and utilization of personal information (OECD, EU)	1	-	1 (0.6)
Personal health information	1	-	1 (0.6)
Law	6	-	6 (3.3)
Privacy information security and medical privacy information security	2	1	3 (1.6)
Integrated medical information system	-	2	2 (1.0)
Multidisciplinary approach	-	1	1 (0.6)
Total ^a (%)	165 (90.2)	18 (9.8)	183 (100)

^aA total of 183 papers. Because, there are more than one objects in 48 papers, and the number of papers increases.

IV. Discussion

There were 48 articles on medical information published in journals from 2005 to 2015 in Korea. Looking at them year by year, one paper was published in 2005, whereas 10 papers

had been published by 2009. However, 38 were published by various academic societies from 2010 to 2015. In terms of research methodology, 33 (68.8%) papers were based on literature review research, while 15 (31.2%) papers reported empirical research. Literature reviews were consistently car-

ried out during the period from 2005 to 2015. However, secondary data analysis was not published. Surveys were published consistently every year; however, in-depth interviews were not conducted during that period. In addition, there has been no report of investigation and experiment in parallel since 2005. Research on medical information systems has been published during this time period, although these papers were fewer than literature review papers.

The results of the theme analysis of papers based on literature review are discussed below. Laws, systems, and policies were the focus of 15 (31.3%) papers. Review discussion and trend topics were the focus of 9 (18.8%) papers. Factor, measures, applications (programs), and utilization topics were the focus of 2 (4.2%) papers each. One (2.1%) paper was published on an actual situation topic. No papers were published on recognition of and satisfaction with medical information security, the effect and influence of medical information security, or model development topics. In empirical research, application (program) topic had 7 (14.6%) papers. Actual situation topic had 4 (8.3%) papers. Law, system, and policy topics had 2 (4.2%) papers. Factor and model development topics had 1 (2.1%) paper each. Recognition and satisfaction, review discussion and trend, effect and influence, measures, or utilization topic had no paper. The lack of prior research focusing on the reliability of medical information and its associated legal issues and the lack of revision of related clause made it difficult to derive a concrete identity policy proposal. Future study should establish a legal concept for the security of medical information. There is a need for more concrete preventive measures and countermeasures against breaches of medical information security through analysis of the reliability of medical information and infringement of platforms. Specific policies that can reduce the number of functional impairments can be proposed by searching for pure functions associated with the use of medical information [6]. Medical information should be protected in compliance with strict confidentiality obligations. It has been proposed that management and supervision with a high level of ethical awareness and the implementation of medical information security system should be the standard practice [9].

For medical information in hospitals where human resources are utilized for various job types and operations, it is important to promote medical information protection in hospitals centering on electronic support. Efforts have been made to improve the level of information protection and information security in medical institutions by establishing measures to protect information, such as the establishment

of administrative measures and countermeasures to have physical security and technical safeguards with information protection policies. It should be emphasized that all staff should take the initiative to make efforts to create a culture that protects medical information [12]. In this study, we analyzed research on medical information security by year, research method, research theme, and research subject. Based on the above analysis results, we found that a systematic approach to research is needed.

Although the scope of personal information has been considered in various fields, including economic, scientific, and technical fields, and this has provided an important foundation for future research, problems such as infringement on the private lives of individuals and society in general have arisen. We need to analyze processes that can handle one or more situations or problems while taking the specialization and specificity of medical information into account [13]. It is necessary to recognize the importance of social awareness of medical information security and its sensitivity. Changes in the perception that health information in the field of medical information technology and policy science should be shared should be prioritized. In recent years, hacking of medical information has been frequently reported. We should actively promote the protection of personal information, curriculum, biographical data, and publications from the viewpoints of research, so we should treat medical information as an important research subject. It is necessary to develop a training program for human resource development. It is also important to build the capacity to strengthen medical information security. In addition, employees of medical institutions are in an important position to protect such information. They should be aware of the importance of medical information; therefore, specific education and training within medical institutions should be provided. It is necessary to develop education programs and continuous education so that employees can increase their awareness of health information protection. In addition, it is important to strengthen internal regulations on the protection of patients' medical information as well as legal regulations [11]. Systematic technology is also needed for medical information security. When a database of medical information and the medical records in a medical information system centered on medical institutions is built, medical information is subjected to advanced persistent threat (APT). Therefore, it is important to consider the vulnerability of and threats to medical information to comply with the Personal Information Protection Law and the Medical Law, and presented security requirements [12]. Legal regulations and government policies also needed

to be specifically established regarding medical information security. The HIPAA (Health Insurance Portability and Accountability Act of 1996) governs the use and disclosure of identification information. It provides specific details applicable to medical insurers, medical staff, and medical information exchange offices that transmit medical personal information in electronic form. The HIPAA also applies to electronically managed and transmitted patient identities, including patient's electronic identification, the information on documents printed from electronic media, and computer systems [8]. It is necessary to standardize inspection items so that they can be applied immediately. Quality management for safe medical information systems is also needed in the field [13]. There should be realistic study of infringement or outflow of medical information or activities related to medical information in the private sector. Through this research, we gained a clearer understanding of the current status of medical information security research in Korea. In addition, this study can be used to help governments, hospitals, and individuals to find ways to protect medical information. There have been many studies on methods, systems, and policies for medical information security. In the future, it will be necessary to try various research methods and conduct practical research on education and inspection related to medical information security.

Conflict of Interest

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

References

1. Council of Europe. Explanatory report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) [Internet]. Strasbourg, France: Council of Europe; c2017 [cited at 2018 Jan 10]. Available from: <https://rm.coe.int/16800ca434>.
2. OECD. Guidelines on the protection of privacy and transborder flows of personal data [Internet]. Paris, France: OECD; c2018 [cited at 2018 Jan 10]. Available from: <http://www.oecd.org/internet/ieconomy/oecd-guidelinesonthe protectionofprivacyandtransborder-flows of personal data.htm>.
3. United Nations. Guidelines for the regulation of computerized personal data files [Internet]. New York (NY): United Nations; 1990 [cited at 2018 Jan 10]. Available from: <http://www.un.org/documents/ga/res/45/a45r095.htm>.
4. Jeun YJ. The medical information protection and major Issues. *J Korea Soc Comput Inf* 2012;17(12):251-8.
5. Kim YR. Exploring the social and legal issues of internet medical information: focusing on the credibility of internet medical information use and invasion of cyber privacy. *J Commun Sci* 2010;10(2):179-220.
6. Jeun YJ. The medical information and privacy protection. *Korean Law Rev* 2006;23:521-40.
7. Lee SM. The medical treatment informatization and medical treatment information protection. *Hanyang Law J* 2006;25(1):39-56.
8. Lee HY. The storage of electronic medical record and trusted third party. *Hanyang Law Rev* 2013;44:123-49.
9. Kim DS, Kim MS. Issues of health information protection and policy direction according to the progress of e-health age. *Informatiz Policy* 2006;13(4):128-48.
10. Lee HJ. Problems and solutions of personal information protection in the medical area. *Korean J Leg Med* 2012; 20(2):267-93.
11. Jung EY, Jung SJ. A study on perception and practice of protecting the patient medical information in some general hospital employees. *Korean J Health Serv Manag* 2014;8(4):35-45.
12. Hong CM, Shin W. Security requirements of order communication system in hospitals for compliance with Personal Information Protection Act. *J Secur Eng* 2013; 10(5):513-26.
13. Jeong HJ, Kim NH. How do they manage personal information in hospital? A survey study for IT governance in hospitals. *Crisisonomy* 2013;9(8):47-66.