https://doi.org/10.33778/kcsa.2019.19.4.123

중소형 의료기관의 개인정보 보안실태 및 개선방안★

신 민 지*, 이 창 무**, 조 성 필***

요 약

급격한 IT 기술의 발달 및 환경의 변화로 새로운 보안 위협이 나타나고 있다. 공격자들은 상대적으로 사이버 범죄 공격의 예방과 방어에 미흡한 의료기관을 대상으로 환자의 민감한 개인정보 유출 공격을 시도하고 있다. 이에 정부는 2016년부터 상급종합병원을 대상으로 ISMS 인증을 의무화하여 의료보안을 강화하고 있지만, 광범위한 보안체계 및 인증은 중소형 의료기관이 수행하기에 한계점이 존재한다. 따라서 본 연구는 중소형 의료기관을 대상으로 관리적, 물리적, 사이버 영역으로 구분하여 의료기관의 개인정보 보안실태 파악 및 개선방안을 도출하고자 하였다. 본 연구의 분석 결과, 중소형 의료기관의 개선방안으로 의료보안 전문인력 투입, 의료보안 교육 및 보안 관리에 대한 지속적인 홍보, 재난·재해에 대비할 수 있는 보호 대책 마련, 중소형 기관에 적합하지 않은 의료정보관리 규정 폐지 및 축소, 정부 차원에서 경제적 지원 및 관리·감독이 필요한 것으로 나타났다.

A Study on the Improvement of Personal Information Protection in Small and Medium-sized Medical Institutions

Shin Min ji*, Lee Chang Moo**, Cho Sung Phil***

ABSTRACT

Rapid developments of IT technology has been creating new security threats. There have been more attacks to get patients' sensitive personal information, targeting medical institutions that are relatively insufficient to prevent and defend against such attacks. Although the government has required senior general hospitals to get the ISMS certification since 2016, such a requirement has been burdensome for small and medium-sized medical institutions. Therefore, this study was designed to draw measures to identify and improve the privacy status of the medical institution by dividing it into management, physical and cyber areas for small and medium-sized medical institutions. The results of this study showed that the government should provide financial support and managerial supervision for the improvement of personal information protection of small and medium-sized medical institutions. They also suggested that the government should also provide medical security specialists, continuous medical security education, disaster planning, reduction of medical information management regulations not suitable for small and medium sized institutions.

Key words : Small and Medium-sized Medical Institutions, Personal Information Protection, Cyber Crime, Personal Information Leakage, Security Measures

접수일(2019년 8월 29일), 수정일(1차: 2019년 9월 19일), 게재확정일(2019년 9월 26일)

★ 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음" (IITP-2019-2014-1-00636*)

* 중앙대학교 대학원 융합보안학과 (제1저자)
** 중앙대학교 산업보안학과 교수 (공동저자)
*** 중앙대학교 산업보안학과 객원교수 (교신저자)

1. 서 론

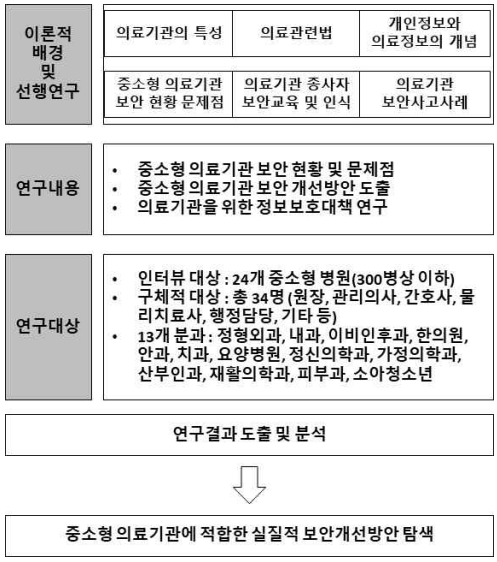
1.1 연구의 필요성

최근 네트워크 기반의 의료기기 발달로 인하여 환자 정보를 포함한 민감한 개인정보들이 네트워크를 통해 수집 · 유통 · 활용되고 있다. 의료기관 뿐만 아니라 보험회사를 포함하여 다양한 기관들이 환자들의 개인정보를 공유하기 때문에 환자의 의료정보 관리 소홀은 환자 개인의 금융기록, 생체정보 등과의 조합을 통해 2차 피해로 이어질 수 있다(김자원, 2018 : 1). 무엇보다도 의료정보는 생명과 신체에 직결되어 있다는 점에서 의료보안의 필요성은 더욱 크다. 하지만 국내 의료보안의 중요성에 대한 인식은 높지 않으며 구체적인 보호 방안도 미흡한 실정이다. 또한, 의료기관 종사자 대부분이 의료정보에 대한 관심도가 낮으며 중요성에 대해 인식하지 못하고 있다(한국보건사회연구원 연구보고서 2013 : 24).

의료기관의 개인정보 유출은 언론 보도를 통하여 쉽게 확인할 수 있을 만큼 빈번히 발생하고 있다. 반면 언론 보도에 따르면, 이에 대응하는 의료기관의 보안대책은 턱없이 부족한 수준이다. 의료정보의 경우 한번 유출되면 회복이 어려운 사정이라는 점에서 그 예방이 무엇보다 중요하다(강지원, 2018 : 1). 하지만 빠르게 변화하는 IT 환경에서 특히 중소형 의료기관들이 보안 위협에 대응하는 데는 재정적인 이유 등 각종 어려움이 수반된다. 실제로 이러한 위협에 대응하기 위한 ISO27799, KISA-ISMS, 스마트 의료보안 가이드라인 등 광범위한 체계는 중소형 의료기관을 포함하여 상급종합병원 또한 적용하기 매우 어려운 실정이다(김양훈, 안병구 2018 : 3, 김자원 2018 : 3). 이처럼 급변하는 의료 환경에서 의료기관 규모에 따른 특성을 고려하여 의료현실에 적합한 실질적 보안 대응이 필요하다. 따라서 본 연구는 개인정보를 중심으로 중소형 의료기관의 특성을 고려하여 의료현실에 적합한 실질적인 보안대책 개선방안을 탐색하고자 한다.

1.2 연구내용 및 방법

본 연구는 중소형 의료기관의 개인정보보호 방안 제시를 위해 의료기관에 대한 이해를 바탕으로 의료기관 보안환경을 분석한 뒤 중소형 의료 환경에 적합한 개인정보 보안 개선방안을 도출하고자 한다. 전체적인 연구모형은 (그림1)과 같다.



(그림 1) 연구모형

※ 출처 : 의료기관을 위한 정보보호 안내서(2016) 재구성

연구방법으로는 문헌연구와 심층 인터뷰를 택하였다. 선행연구를 통하여 의료기관의 특성을 파악 후 보건복지부가 발행한 의료기관을 위한 정보보호 안내서(2016)를 참고하여 심층 인터뷰 문항을 작성하였다. 연구대상은 24개의(300병상 이하) 중소형 병원으로, 총 34명을 심층 인터뷰하였으며, 다양한 의견을 수집하고자 13개의 분과를 대상으로 인터뷰를 진행하였다. 인터뷰 문항으로는 개인정보에 대한 인식의 정도, 의료기관에서 개인정보 유출 피해 경험, 근무하는 의료기관에서 보안 관리현황을 조사하였다. 보안 관리현황은 관리적, 물리적, 사이버 영역으로 구분하여 면담을 진행하였다. 이를 바탕으로 현재 중소형 의료기관에서 개인정보 보안 관리의 문제점과 효과적인 개선방안

을 알아보고자 하였다.

인터뷰는 의료보안에 대한 전반적 지식과 이해도를 가진 병원 관계자를 대상으로 1인당 1회씩 인터뷰를 진행하였다. 지역적 차이의 의견을 반영하기 위하여 서울, 경기지역을 대상으로 나누어 진행하였으며 300병상 이하의 규모인 중소형 병원을 선정하였다. 의사, 간호사, 행정직 의료기관 종사자를 모두 포함하여 중소형 의료기관에서의 보안 관리현황을 파악하고 중소형 의료기관에 적합한 실질적인 보안개선 방안을 찾고자 하였다.

인터뷰 진행은 2019.07.25부터 2019.08.03.까지 진행하였다. 면담을 진행하기에 앞서 사전에 연구참여자에게 인터뷰 항목에 대하여 공지하였다. 면담 내용은 개방형 질문을 시작으로 세부적 질문으로 좁혀 들어갔다. 상세 인터뷰 문항에 관한 내용은 병원 내 보안부서의 유무, 의료보안 사고 여부, 의료보안의 필요성을 비롯한 중소형 의료기관에 적합한 보안개선 방안에 대하여 인터뷰하였다. 인터뷰 내용 모두 한글 프로그램을 통하여 전사하였으며 개인정보와 관련한 내용은 제외한 후 논문에 인용하였다.

2. 이론적 배경 및 선행연구

2.1 이론적 논의

2.1.1 의료기관의 정의 및 분류

의료기관이란 의료인이 공중(公衆) 또는 특정 다수인을 위하여 의료·조산의 업(이하 "의료업"이라 한다)을 하는 곳을 말한다(의료법 제3조 1항). 의료기관의 규모는 의원급, 조산원, 병원급 의료기관으로 나누어진다. 의원급은 외래환자를 대상으로 의원, 치과의원, 한의원으로 나누어진다(의료법 제 3조). 병원급은 입원환자를 대상으로 병원, 치과병원, 한방병원, 요양병원, 종합병원으로 구분한다(의료법 제 3조 3항). 병원, 치과병원, 한방병원 및 요양병원은 30개 이상의 병상을 보유하며, 종합병원은 100개 이상의 병상을 보유한다.

종합병원은 종합병원과 상급종합병원으로 분류된다. 상급종합병원은 보건복지부 장관이 일정 요건을 갖춘 종합병원 중에서 중증질환에 대하여 난이도가 높은 의료행위를 전문적으로 하는 종합병원을 상급종합병원으로 지정할 수 있다.

<표 1> 의료법에 따른 의료기관 분류

구분	설명	종류	
의원급	외래환자 대상	의원	
		치과의원	
		한의원	
조산원	임산부 및 신생아 대상	-	
병원급	입원환자 대상	병원 (30개 이상의 병상)	
		치과병원 (30개 이상의 병상)	
		한방병원 (30개 이상의 병상)	
		요양병원 (30개 이상의 병상)	
		종합병원 (100개 이상의 병상)	종합병원
			상급종합병원

2.1.2 중소형 의료기관의 범위설정 및 특징

현재 중소형 의료기관에 대한 정의는 법률적으로나 학문적으로 명시된 공식적인 용어는 아니다. 하지만 의료 전달체계나 정책 측면에서는 광범위하게 사용되고 있다. 또한, 우리나라에서 중소병원에 대한 정의는 학자마다 의견이 다르고 각 단체에 따라 명확하게 정의되지 않은 채 사용되고 있다(김성협, 2002 : 17).

김자원(2017)은 일반병원과 의원을 대상으로 중소형 의료기관의 범위를 설정하였다. 이난경 · 이종옥(2015)은 대형병원과 대립하는 개념으로 통상 300병상 이하 또는 500병상 이하인 병원으로 지칭하였다. 한기성(2012)은 대한중소병원협의

회를 기준으로 100병상 이상 500병상 미만으로 중소형 의료기관을 정의하였으며, 김상한(2004)은 인턴· 주요 과목 레지던트 수련병원이거나 300병상 이하에 해당한다고 정의하였다. 김성협(2002)은 300병상 이하의 병원 및 종합병원급 의료기관을 중소병원으로 바라보았다.

선행연구를 통하여 중소형 의료기관의 범위를 살펴본바, 대형병원과는 대립 되는 개념으로 주로 의원과 일반병원에 해당하며 통상 300병상 이하의 병상 수를 갖는 것으로 보인다. 통계청(2019) 자료를 토대로 의료기관 현황을 살펴보면, 의원 30,532개소, 일반병원 1,370개소, 종합병원 341개소, 요양병원과 특수병원을 포함한 전문병원은 1,555개로 나타났다. 본 논문에서는 중소형 의료기관의 범위를 전체 33,798개소 의료기관 중 31,902개소(약 93.39%)를 차지하는 의원과 일반병원을 대상으로 설정하였다. 다음은 중소형 의료기관의 특징을 살펴보고자 한다. 중소형 의료기관은 대형병원에 대비되는 개념으로서 보건의료체계와 제도상의 문제를 복합적으로 가지고 있으면서 정책적 지원이 필요한 의료기관으로 받아들여지고 있다(한기성, 2012 : 4). 본 논문에서 통계청에서 중소형 의료기관의 수를 살펴본 결과, 중소병원은 병원 산업에서 많은 수를 차지하고 있다. 또한, 지역 주민들에게 편리한 의료이용을 가져다줌과 동시에 간접비용을 경감시켜준다.

환자의 개인정보와 진료 정보로 이루어진 의료정보는 홈페이지, OCS(Order Communication System), EMR(Electronic Medical Record), PACS(Picture Archiving Communication System) 4가지로 구분되어 병원정보시스템으로 관리되고 있다(안선주 2016 : 38). 이처럼 의료기관의 정보화를 통하여 공유되는 환자 정보는 의료기관 간 정보를 전달하고 공유하게 된다. 특히 국내의 의료전달체계 중 중소형 의료기관에서 상급종합병원에서 진료를 받게 될 경우, 진로 효율성 향상 및 진로 비용 절감을 위하여 중소형 의료기관에서 생성된 진료 정보를 재활용하게 된다(한성화, 2017 : 2). 이때 진료 정보를 전달하는 과정에서 의료정보가 평문으로 전송될 때 환자의 정보가 노출될 수 있다. 이 경우 환자의 개인정보 유출뿐만 아니라 정보의 무결성 침해로 인한 부정확한 정보로 위험을 의료 보안사고 발생은 의료기관의 조직 평판 및 신뢰도 하락의 위험이 발생한다(김동수·김민수, 2007 : 3). 이와 같은 문제를 해결하기 위하여 2018년도 스마트 의료보안 가이드라인이 나왔지만 광범위한 체계는 중소형 의료기관에 적용하기 한계가 있다. 이에 본 논문은 중소형 의료기관에 적합한 보안 개선방안을 탐색하고자 한다.

2.1.3 개인의료정보의 개념 및 유출사례

현행법 중 개인의료정보에 대한 명확한 정의를 규정한 것은 없다. 학자마다 개인의료정보에 대한 정의를 다르게 표현하고 있다. 정규원(2011)에 의하면 의료정보는 환자의 진료 과정에서 얻어진 환자의 사적인 부분을 포함하는 자료를 의미한다. 김성찬(2002)은 의료정보는 의료의 제공을 위하여 진료를 통해 얻은 환자의 건강상태나 평가로 서류 등의 매체를 통하여 기록된 정보를 말한다. 김강한(2016)은 의료정보를 건강정보로 칭하고 건강을 유지하는데 필요한 건강에 대한 정보로써 개인신상정보, 개인의료정보를 모두 포괄하여 바라보았다. 이 외에도 학자마다 개인의료정보에 대한 개념이 명확하게 정의되어 있지 않아 의료정보, 개인의료정보, 개인 건강정보, 보건의료정보 등 혼용되어 사용되고 있다.

본 논문에서는 개인의료정보에 대한 개념을 진료를 통해 얻은 환자에 관한 모든 기록으로 정의하였다. 의료정보는 일반적인 개인정보보다 민감한 정보를 포함하며 다양한 내용의 조합을 통해 더 큰 피해로 이어질 수 있다. 따라서 의료정보에 대한 정확한 개념 정의가 필요하며 수집에 있어 엄격한 관리와 규제가 필요하다. 앞서 설명한 의료기관의 미흡한 보안 수준과 의료전달 체계로 인한 유출로 인하여 의료기관 개인정보 유출이 발생한다. 다음 <표 2>는 최근 5년간 의료기관에서 발생한 개인정보 유출사례이다.

<표 2> 의료기관에서 개인정보 유출사례

일시	내용
2015.08.12	북한의 해킹공격으로 대형 대학병원 전산망을 해킹해 환자의 개인정보 유출[24]
2016.08.30	비밀번호를 단순 대입하는 방법으로 산부인과와 성형외과 홈페이지를 해킹해 1만6,000여 건의 개인정보로 SNS 계정 도용[25]
2016.07.18	미국 빅데이터 기업에 흘러가 한국 4,300만 명의 개인의료정보[26]
2016.10.06	대학병원 교수 리베이트 위해 환자 개인의료정보 29만 건 제약업체에 제공[27]
2018.10.05	치과병원 환자의 핸드폰 번호를 포함한 개인의료정보 1천여 건, 3개월간 페이스트빈에 노출[28]
2018.11.09	의료진이 환자의 개인정보를 무단 열람하여 환자의 개인정보를 외부로 유출하여 벌금형, 기소유예 처분[29]
2019.01.15	대형 의료기관에서 공채 지원자 150여 명 이메일 주소 노출[30]

의료기관의 개인정보 유출을 넘어 의사가 사용하는 PC를 조작하여 처방전을 바꿔치기하거나 약물 투여량 변경을 통하여 의료사고를 유발할 수 있다. 이처럼 의료기관이 해킹에 노출되는 것은 개인정보 유출 사고를 넘어 생명과 직결된 중요한 문제이다. 의료기관을 대상으로 한 보안 위협이 계속해서 발생하고 있지만, 의료기관의 특성을 반영한 정보보안체계는 이루어지지 않고 있다(김양훈, 안병구 2018 : 4). 특히 대형 의료기관에 비해 인적·경제적으로 한계가 있는 중소형 의료기관을 위한 보안대책 마련이 시급하다.

2.2 선행연구

중소형 의료기관을 대상으로 한 개인정보 보안실태 및 개선방안에 관한 선행연구는 찾아볼 수 없었고, 주로 대형 의료기관으로 한 보안 관리 실태와 관리방안을 제시한 논문이 대부분이었다. 본 논문은 중소형 의료기관에 대한 특성과 개인의료정보에 대한 개념을 선행연구로 참고하였으며, 이를 바탕으로 중소형 의료기관 특성을 반영한 개인정보 개선방안을 제시하고자 한다.

분석한 선행연구를 재분류해보면 중소형 의료기관, 개인의료정보, 의료보안 위협 및 개선방안으로 정리해 볼 수 있다. 우선 중소형 의료기관에 관한 선행연구로 김양훈·안병구(2018)는 중소형 의료기관을 중심으로 보안체계구축 분석과 함께 보안체계를 제시하였다. 김자원(2017)은 중소형 의료기관을 대상으로 보안 관리 평가 항목을 설계하였다. 이난경·이종옥(2015)은 IT 기반에 따른 의료서비스 발달에 따라 중소형 병원의 클라우드 서비스 모형을 제시하였다.

개인의료정보에 관한 선행연구로 박정홍(2017)은 개인 의료 정보보안에 대한 설문조사로 의료서비스의 편의성을 향상한다는 연구결과를 도출하였다. 김한나 외 4명(2013)은 국내 의료정보보호 법제 분석과 함께 개인의료정보 관리 및 보호 방안에 대하여 제시하였다. 정영철·이기호·이야리(2013)은 의료기관에서 개인정보보호 관련 정책 현황 조사와 함께 국내 개인의료정보보호에 대한 인식 조사를 시행하였다. 이한주(2012)는 단계별로 일어날 수 있는 의료정보보호 개념 정립 및 문제를 검토하였다. 마지막으로 의료보안 위협 및 개선방안으로 김양훈·장항배(2018)은 의료정보 생애주기를 제시하며 단계별 보안 위협과 대응방안을 제시하였다. 노시춘·최진탁(2013)은 U-Healthcare 네트워크 보안 프레임워크 설계를 통하여 의료정보의 취약성을 진단하고 그에 맞는 대책 방안을 제시하였다. 송유진·박광용(2010)은 의료데이터 공유 및 활용과정에서 발생하는 문제점과 보안 제안사항에 대해 제시하였다.

이러한 선행연구를 분석하여 보았을 때 IT 기반 의료서비스 발달과 의료 전달체계 특성에 따라 보안 위협이 존재하며 단계별에 맞는 보안대책이 필요한 것으로 보인다. 특히 대형병원에 비교하면 중소형 의료기관은 경제적인 부담으로 보안 관리를 실행하기에 한계점이 존재한다. 이에 본 연구는 중소형 의료기관을 대상으로 개인정보 보안실태를 파악하고 실질적이고 경제적인 보안 개선방안을 제시하는 데 목적을 두고 있다.

3. 중소형 의료기관의 개인정보 보안실태

3.1 중소형 의료기관 개인정보 보안 현황

본 연구는 중소형 의료기관의 개인정보보호 방안 제시를 위해 24개의 중소형 의료기관 13개 분과를 대상으로 인터뷰를 진행하였다. 인터뷰 결과, 병원 종사자들 대부분이 개인정보보호의 필요성에 대해 인식하고 있었으나 전담인력 부족 및 경제적인 부담으로 인하여 기본적인 보안 관리조차 실행되지 않고 있었다. 인터뷰 문항으로는 중소형 의료기관 개인정보 보안실태를 파악하고자 관리적, 물리적, 사이버 영역으로 구분하여 보안실태를 파악하고자 하였다.

관리적 보안 관리현황

“병원 보안규정과 관련된 정책도 수립되어 있지 않고 보안교육도 한 번도 받아 본 적이 없어요. 의료보안에 대해 중요하다고 생각하지만, 중소형 병원이 보안까지 신경 쓰기에 업무량도 만만치 않고 경제적으로도 부담이 커요.”(치과 원장)

“의료보안에 대한 필요성을 느껴 온라인 의료보안 교육을 수강한 경험이 있는데, 온라인 강의에 한계점을 많이 느꼈어요. 저는 보안을 전공으로 하지 않아서 재미도 없고, 무엇보다 이해하기 쉽지 않았어요.”(정형외과 원무행정)

“진료접수 시 환자의 생년월일, 전화번호, 성함 등 개인정보를 구두로 확인 시 진료 대기 중인 환자에게 환자의 개인정보 유출이 걱정될 때도 있어요. 또한, 환자 보호자가 찾아와서 무리하게 환자차트 복사를 계속 요구할 시 난감한 경우도 여럿 있어요.”(이비인후과 원장)

물리적 보안 관리현황

“병원 직원 모두가 개인정보보호 필요성에 대하여 인식하고 있어요. 하지만 병원 업무가 너무 바쁘다 보니 보안에 신경 쓸 수 없어요. 또한, 우리 병원은 종이차트로 된 환자 정보를 별도의 잠금장치 없이 보관하고 있으며 출력물 파기도 제대로 하지 못하고 있어요.”(피부과 병원장)

“개인정보가 포함된 서류를 종이차트로 보관하고 있어요. 하지만 보관할 장소가 넉넉하지 못하여 잠금장치가 설치된 곳에 보관하고 있지는 못해요.” (가정의학과 원장)

“재해로부터 보호하기 위한 보호 대책은 따로 수립되어 있지 않아요. 시스템 장애 시 대체할 수 있는 예비 장비를 도입하기에 예산이 부족해요.”(내과 원장)

사이버 보안 관리현황

“보험회사 직원이 진료 기록지 사본을 요청할 때나 내부직원 사직 시 개인정보 유출이 걱정돼요. 또한, 원장을 포함한 병원 직원들은 컴퓨터에 익숙하지 못해요. 그러다 보니 파일을 암호화하여 환자의 개인정보를 보호하는 등 기술적인 조치는 부족해요.”(내과 병원장)

“바이러스 PC 검사는 가끔 한 번씩 하기는 하는데.. 개인정보 파일 암호화는 어떻게 하는지 잘 모르겠어요. 컴퓨터 계정 비밀번호를 주기적으로 바꾸면 혼동되기도 하고 까먹어서 변경하지 않는 편이에요.”(한의원 원장)

중소형 의료기관 인터뷰를 통하여 관리적, 물리적, 사이버 분야별로 개인정보 보안실태를 파악하였다. 의료기관 대부분 개인정보보호의 중요성을 인식하였지만, 구체적인 보안 대처방안에 대해서는 인식하고 있지 못하였다. 또한, 경제적인 부담으로 중소형 병원에서 별도로 보안 관련 부서 및 전담인력은 존재하지 않았으며 보안교육을 경험한 병원도 극히 일부였다. 병원 직원들 대부분 컴퓨터에 익숙하지 못하여 적절한 사전예방 조치에 미흡한 것으로 확인되었다.

3.2 중소형 의료기관의 개인정보 보안관리 개선 제안사항

앞서 중소형 의료기관의 개인정보 보안실태 파악을 통하여 중소형 의료기관은 전담인력 부족 및 경제적 부담으로 보안 관리를 실행하기 한계점이 있는 것을 확인할 수 있었다. 이에 본 연구는 중소형 의료기관을 대상으로 관리적, 물리적, 사이버 영역으로 구분하여 중소형 의료기관에 적합한 개인정보 보안 관리 제안사항에 관한 의견을 도출하고자 한다.

관리적 보안

“보안교육을 통해 개인정보 보안에 대한 관심을 갖게 하고 사전예방을 통하여 정보 유출을 막아 개선할 수 있다고 생각해요. 개인정보보호가 중요하다고 생각하지만, 막상 어떻게 보안을 해야 할지 방법을 몰라 실천하지 못하는 경우가 많아요. 사례중심의 구체적 실천방안을 통하여 온라인 교육이 제공되면 좋겠어요.”(소아청소년 원장)

“과도한 의료정보관리 규정을 폐지하거나 축소하여 중소형 의료기관에서도 관리 할 수 있는 수준으로 개선하였으면 해요. 현재 중소형 병원의 의료관련 정보의 중요성 정도를 살펴볼 때 병원의 규모에 맞는 의료정보 보안 관리 규정을 다시 설정할 필요가 있어 보여요.”(재활의학과 병원장)

“환자의 개인정보가 유출되면 안된다는 강조는 많이 들었지만, 구체적인 교육이나 자세한 리스트는 없었어요. 6개월마다 한 번씩 오프라인 강의를 수료하고 평가하여 기준점에 미치지 못하는 사람들은 추가로 3개월에 한 번씩 더 실시하면 좋을 것 같아요. 평가 후 핸디캡을 줘야 어떤 형태의 경각심이 든 기억에 남을 것 같아요”(정신건강의학과 직원)

“의료인 보수교육은 매년 온라인으로 이수해야 하는데, 개인정보 보안 관리에 대한 과목을 신설되면 좋을 것 같아요.”(한의원 원장)

물리적 보안

“병원 공간이 협소해서 별도 공간을 마련하여 많은 서류보관을 하기 힘들어요. 따로 정부 차원에서 시·도·구 별로 오랫동안 보관해야 할 출력물을 보관할 장소를 마련해준다면 안전하게 관리 할 수 있을 것 같아요.”(안과 원장)

“파쇄하지 못하고 쌓여 있는 문서가 꽤 있어요. 처리도 어렵고... 경제적으로 여유가 있는 중소병원은 문서파쇄업체와 계약을 맺어 처리하는데, 우리 병원은 그럴만한 여유가 없어요. 이를 위해 개인 의원 보안 관리에 정부 차원의 경제적 지원이 필요해요.”(이비인후과 병원장)

사이버 보안

“컴퓨터에 백신 프로그램이 설치되어 있기는 하지만 정기적인 점검이 필요해요. 컴퓨터를 잘 모르니 보안 전문인력이 방문해서 정기적으로 컴퓨터 점검을 해주었으면 좋겠어요. 보안을 하고 싶어도 어떻게 하는지 방법을 모르는 사람이 더 많을 것 같아요. 또는 중소형 병원을 위한 보안 관리 관련된 필요한 정보들을 포스터에 적어 배부해준다면 필요할 때 찾아보고 문제를 쉽게 해결할 수 있을 것 같아요.”(이비인후과 간호사)

“우리 병원에서 컴퓨터를 능숙하게 잘 다루는 사람이 없다 보니, 사용 중에 컴퓨터가 고장 나면 외부업체에 맡겨요. 수리업체에 환자들의 개인정보가 노출될까 걱정돼요. 해결방안으로는 의료기관을 위한 프로그램 툴 개발을 하면 좋을 것 같아요. 또는 정부 차원에서 의료기관의 컴퓨터를 관찰하여 위험을 감지하고 문제가 있다면 사전 예방할 수 있게 공지를 해주거나 원격으로 조정하여 문제를 해결해줬으면 좋겠어요.”(정형외과 원장)

“중소형 의료기관은 직원의 수가 적고 여러 가지 업무를 한사람이 맡아 하는 경우가 많아 보안에 신경 쓰기 어려워요. 보안교육으로 인식개선은 가능하겠지만 인식개선만으로는 해결될 문제는 아닌

것 같아요. 그저 말뿐만인 교육이 아니라 전문인력의 방문으로 각 의료기관의 시스템을 점검하고 문제점이 무엇인지, 어떻게 개선되어야 하는지에 대한 구체적인 방안을 제시하고 유지할 수 있도록 지속적인 관리·감독이 필요하다고 생각해요. 개인정보가 중요하다고 하지만 제대로 감독하지 않는 관리기관의 문제가 가장 크다고 생각해요."(재활의학과 물리치료사)

인터뷰를 통한 중소형 의료기관의 개인정보 보안 제안사항 의견을 도출하면 다음과 같다. 먼저, 관리적 분야에서 보안 관리 제안사항이다. 의료보안교육에 대한 필요성으로 의료보안의 중요성을 깨닫고 개인정보 보안을 개선하려 해도 구체적인 실천방법을 몰라 하지 못하는 경우가 대부분이었다. 따라서 온라인·오프라인 교육을 통하여 보안사고 사전예방 교육 및 대처방안 교육이 필요하다. 그저 시간 채우기 교육이 아닌 사례 중심의 구체적 실천방안 교육이 필요하다는 의견이다.

다음은 물리적 분야에서 보안 관리 제안사항이다. 중소형 병원은 환자의 개인정보를 포함한 중요문서를 관리하기에 경제적·공간적 여유가 부족하다. 이에 대한 해결책으로 중요문서를 보관할 장소 대여 등 개인 의원 보안 관리에 정부 차원의 경제적 지원이 필요하다. 또한, 각종 재난·재해에 대비하여 안전한 보호 대책을 마련해야 한다.

마지막으로 사이버 분야에서 보안 관리 제안사항이다. 보안환경 개선을 위한 노력에도 불구하고 원장을 포함한 직원 대부분은 컴퓨터 및 보안에 전문지식이 부족해 실행하기 어려운 실정이다. 중소형 의료기관은 직원 수가 적고 한사람이 여러 가지 업무를 맡아 보안까지 신경 쓰기 힘들다는 의견이 많았다. 이를 위해 의료보안 전문인력을 투입해 정기적으로 방문하여 점검이 필요하다.

4. 중소형 의료기관의 개인정보 보안 개선방안

본 연구는 중소형 의료기관의 개인정보 보안실태를 파악하고 제안사항을 분석하여 중소형 의료기관에 적합한 개선방안을 도출하였다.

관리적 개선방안으로 의료보안 교육 및 보안관리에 대한 지속적인 홍보가 필요하다. 의료기관 종사자도 보안사고에 대응 가능한 실질적 교육을 통하여 사전예방 교육이 필요하며, 의료보안 분야에 대한 지속적인 관심과 홍보가 필요하다. 또한, 중소형 기관에 적합한 의료정보관리 규정 폐지 및 축소가 이뤄져야 할 것이다. 경제적 부담 및 전담인력 부족으로 중소형 의료기관이 실행하기에 광범위한 보안 관리체계는 무리가 있기에 적합한 의료정보관리 규정 개선이 필요하다.

우선 각종 위험으로부터 개인정보를 보호할 수 있는 물리적 보안 방안을 마련해야 할 것이다. 개인정보를 보관하는 장소와 장비에 대한 출입통제 노력을 강화하고, 시건장치 점검 등 물리적 보안 개선 활동이 선행돼야 한다고 보인다. 이를 위해, 환자의 개인정보가 담긴 종이차트를 보관할 공간적 여유가 부족한 중소형 의료기관을 대상으로 별도의 장소 마련이 필요하다. 또한, 물리적 자산 이송 시 파손, 훼손, 도난의 위험으로부터 보호 대책을 수립해야 한다.

사이버 개선방안으로 의료보안 전문인력 투입이 필요한 것으로 보인다. 교육만으로 해결할 수 없는 문제가 존재하기에 정기적으로 기술 전문인력을 투입하여 철저한 관리·감독이 필요하다.

무엇보다도 중소형 의료기관의 경우, 개인정보 보호에 충분한 인적, 재정적 투자를 하기 어려운 실정이다. 따라서 정부 차원에서 보안 활동을 수행하기 어려운 개인 의원 등 중소형 의료기관을 대상으로 정부 차원에서 적극적인 경제적 지원이 시급하다고 여겨진다.

5. 결 론

본 논문은 중소형 의료기관의 의사, 간호사 등 관련 종사자에 대한 인터뷰를 통하여 중소형 의료기관의 개인정보에 대한 인식의 정도를 파악하고자 하였다. 인터뷰 문항의 내용으로는 개인정보에 대한 인식, 개인정보 유출 피해 여부, 병원 내 보

안부서 유무를 비롯하여 보안 관리현황을 파악하기 위하여 관리적·물리적·사이버 보안 관리 영역을 나누어 인터뷰를 진행하였다. 인터뷰 결과 중소형 의료기관은 환자의 개인정보보호 필요성은 인식하고 있었으나 경제적 어려움 및 전담인력 부족으로 보안 활동 수행에 있어서 어려움을 겪고 있다.

각 영역에 대한 제안사항을 분석하였을 때, 무엇보다도 가장 중요한 것은 정부 차원에서 지속적인 관리와 경제적인 지원이다. 중소형 의료기관은 전담인력 부족 및 경제적 투자의 한계로 환자의 개인정보보호를 위한 사전예방 조치 및 보안대책 방안 수립에 미흡한 것으로 확인되었다.

제안사항을 분석으로 중소형 의료기관에 적합한 개선방안을 도출하였다. 개선방안으로는 의료보안 교육 및 보안 관리에 대한 지속적인 홍보, 중소형 기관에 적합한 의료정보관리 규정 폐지 및 축소, 재난·재해에 대비할 수 있는 보호 대책 마련, 기술보안 전문인력 투입이다. 현재 중소형 병원의 의료관련 정보의 중요성 정도를 살펴볼 때, 병원의 규모에 맞는 의료정보 보안 관리 규정과 정책을 재설정해야 한다. 2016년부터 대형병원은 ISMS 인증이 의무화되어 시행되고 있다. 이에 발맞춰 한국인터넷진흥원에서 발행한 의료보안을 위한 가이드라인은 관리적, 물리적, 사이버 광범위한 관리체계는 대형병원에서도 모두 갖추기에 무리가 있으며 중소형 의료기관 역시 적용하기 어려운 실정이다. 따라서 중소형 기관에 적합한 의료정보관리 규정 설정이 필요하다.

본 연구는 중소형 의료기관의 개인정보 보안실태 및 개선방안을 토대로 더 나은 중소형 의료기관의 보안환경 개선을 도모하는데 이바지할 수 있을 것으로 기대한다. 다만, 본 연구는 중소형 의료기관의 대상이 부분적이어서 연구결과를 일반화하기 어렵다. 이는 후속연구를 통해 연구의 한계점을 보완해야 할 것이다.

참고문헌

[1] 강지원, “병원 간호사의 의료정보보안 측정도구 개발,” 고려대학교 대학원 석사학위논문, 2018.

[2] 김강한, “개인건강정보보호에 관한 헌법적 고찰: 공공영역에서의 개인건강정보보호를 중심으로,” 아주법학 제 10권 제 2호, pp. 1-40, 2016.

[3] 김동수, 김민수, “u-Health 환경에서의 정보보호 수준제고를 위한 보안 표준 개발,” 대한산업공학회 제 2권, pp. 177-185, 2007.

[4] 김보경, 김수진, 김정덕, “의료산업에서의 정보보호를 위한 고려사항”, 한국 IT 서비스학회 학술대회 논문집, pp. 299-303, 2016.

[5] 감상한, “병원의 서비스품질이 고객 만족과 성과에 미치는 영향에 관한연구: 중소병원을 중심으로,” 경희대 석사학위논문, 2004.

[6] 김성찬, “영미법상 의료정보에 대한 환자의 엑세스권,” 법과 정책 제8호, 제주대학교 사회발전과 법, 정책연구소, pp. 17-32, 2002.

[7] 김성협(2002), “중소병원의 정보화 전략에 관한 연구, 인천대학교 석사논문,” 2002.

[8] 김양훈, 안병구, “의료융합 환경에서 수용성을 고려한 비용 효율적 보안체계구축 방안 연구 : 중소의료기관을 중심으로,” 융합보안논문지 제 5권, pp. 75-81, 2018.

[9] 김양훈, 장항배, “미래 환경변화와 의료보안 과제,” 한국컴퓨터통신연구회 제 2권, pp. 4-9, 2018.

[10] 김자원, “중소형 의료기관을 위한 보안관리 평가모형 설계 연구,” 중앙대학교 대학원 석사학위논문, 2018.

[11] 김한나, 이얼, 김계현, 이정찬, 이평수, “개인의료정보의 관리 및 보호방안,” 대한의사협회 의료정책연구소 연구보고서 pp. 1-143, 2013.

[12] 노시춘, 최진탁, “u-Healthcare 의료정보 시스템 네트워크 보안프레임워크 설계방법,” 융복합지식학회논문지 제 1권, pp. 31-37, 2013.

[13] 박인경(2006). 개인의료정보보호에 관한 법적 연구, 연세대학교 대학원 석사논문.

[14] 박정홍, “개인의료정보보안인식이 편의성에 미

치는 영향," 한국콘텐츠학회논문지 제 6권, pp. 600-612, 2017.
[15] 백윤철, "우리나라에서의 의료정보와 개인정보 보호," 헌법학연구 제 11권 제 1호, pp. 395-442, 2005.
[16] 송유진, 박광용, "의료데이터 공유 및 활용 서비스를 위한 보안/프라이버시 요구사항," 한국정보보호학회 제 3권, pp. 90-96, 2010.
[17] 안선주, "2016 표준기반 R&D 로드맵_스마트헬스," 국가기술표준원(KATS), 한국표준협회(KSA), 2016.
[18] 이난경, 이종옥, "중소형 병원의 클라우드 병원정보시스템 서비스 체계에 관한 연구," 한국전자거래학회지 제 20권 제 3호, pp. 89-112, 2015.
[19] 이한주, "의료영역에서의 개인정보보호의 문제점과 해결방안," 한국의료법학회지 제 20권 제 2호, pp. 267-293, 2012.
[20] 정영철, 이기호, 이야리, "의료기관의 개인정보 보호 현황과 대책," 한국보건사회연구보고서, 2013.
[21] 한기성, "중소병원 정보시스템의 아웃소싱 결정요인에 관한 연구," 경원대학교 석사학위논문, 2012.
[22] 한성화, "의료기관 간 의료정보 전송 보안체계 개선방안에 관한 연구," 동국대학교 대학원 석사학위논문, 2017.
[23] 황지환, "의료기관의 개인정보 보호의 현황과 향후 개선방안," 의료정책포럼 제 14권 제 4호, pp.55-61, 2017.
[24] http://www.hankookilbo.com/News/Read/201508121938897224
[25] http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201608302259015
[26] http://www.hani.co.kr/arti/economy/it/752750.html
[27] http://www.rapportian.com/news/articleView.html?idxno=28898
[28] https://www.boannews.com/media/view.asp?idx=73433
[29] https://news.kbs.co.kr/news/view.do?ncd=4070088
[30] http://www.newspim.com/news/view/20190115000428

〔저 자 소 개〕

신 민 지 (Min-ji Shin)
2018년 ~ 현재 중앙대학교 융합보안학과 석사과정

email : shinminji1995@gmail.com

이 창 무 (Chang-moo Lee)
2002년 뉴욕시립대 형사사법학 박사
2014년 ~ 현재 중앙대학교 산업보안학과 교수

email : cmlee@cau.ac.kr

조 성 필 (Sung-phil Cho)
2014년 한양대학교 정보시스템 박사
2018년 ~ 현재 중앙대학교 산업보안학과 객원교수

email : okland2002@naver.com