원 저

의료기관의 정보보호교육과 정보보안생활과의 관련성

김종덕*, 홍화영*, 김재현*

*단국대학교 일반대학원 보건학과 보건행정학전공

〈Abstract〉

Relationship between Information Security Education and Information Protection Practice of Hospital

Jongdeok Kim*, Hwayong Hong*, Jae-Hyun Kim*

*Department of Healthcare Administration Dankook University College of Health Science

PURPOSE: To demonstrate that the training of information protection for members at medical institutions increases the information protection activities of employees.

METHODS: We used the chi-square test and the logistic regression model to analyze the data of the "Healthcare Information and Communication Status Survey in 2017" (n = 2002) conducted by the Korea Health Industry Development Institute

RESULTS: As a result of the analysis, the information protection activity increased when the education was received and the number of received more than the education was not received. Especially, when the management receives education, it affects the information protection activities of the employees.

CONCLUSION: In order to protect medical information, medical institutions need to provide education on information protection for management and employees.

Key Word : Hospital, Information Protection, Information Security Education, Information Protection Recognition, Information Protection Practice

Ⅰ. 서 론

'개인정보'에 대한 정의는 개인정보보호법에서 규정하고 있으나, '개인의료정보'는 특별한 규정 없이 개인정보보호법에 건강, 성생활 등에 관한 정보를 포함하여 '민간정보'로만 규정하고 있다.[1]

일반적으로 '개인의료정보'는 개인정보 중 국민의 건강을 보호하고, 증진하기 위하여 의료인과 의료기관 등이 행하는 의료행위와 관련된 정보를 의미하는 것[2]으로 개인정보와 다른 몇 가지 특성이 있다.

의료정보는 환자가 의료기관을 방문하여 진료를 통해 생성되어 의료기관에서 환자와 접촉하는 의료기관 종사자는 정보주체의 개인의료정보에 대한 접근과 이용이 가능하다는 점[3]과 법에 따라 제3자에게 제공할 수 있고 제공 받은 기관은 개인의료정보를 제공 받은 목적 범위 내에서 사용할 수 있다는 점4[4]과 전문적 지식 경험 기술과 결합된 특성을 지닌5[5] 질병 및 유전정보 등의 정보로 일반 개인정보와 비교하여 심각한 사생활 침해가 발생할 수 있으며[6] 한 번 유출 되면 다시 원상회복이 어려운 특성이 있다.[7]

* 투고일자 : 2019년 4월 23일, 수정일자 : 2019년 6월 8일, 게재확정일자 : 2019년 6월 26일

† 교신저자 : 김재현, 단국대학교 보건행정학과, Tel : 041-550-1472, Fax : 041-559-7934, E-mail : jaehyun@dankook.ac.kr

아울러, 4차산업혁명시대 의료영역에서도 IT기술이 접목되어 개인의 의료 관련 정보가 대량으로 입력 처리되어 데이터베이스화 되고, 환자 진료의 연속성 지원을 위해 다른 의료기관과의 진료정보가 공유할 수 있다는 점[8], 정보를 제3자 제공할 수 있어 제3자도 개인의료정보에 대한 접근 및 이용[1] 하는 등으로 의료정보가 교류 활용 되고 있어 오 남용 및 유출 등 개인의 프라이버시 침해 가능성이 높아지고 있는 상황에서[9] 정보 유출의 위험성에 대한 문제 제기가 꾸준한 이어지고 있는 상황이다.[10]

의료기관은 정보보호를 목적으로 조직 내 정보 자산의 보안을 위해 구현한 관리 장치로서 기술적, 물리적 장치뿐만 아니라 관리적 장치를 포함해 다차원적인 구성을 통해 정보보호활동[11]해 왔으나, 침입탐지시스템(IDS : Intrusion Detection System)의 효과를 기대[12]하거나 컴퓨터 바이러스 감염 감소에 기여한다는 정보보호 S/W 사용[13] 등의 시스템을 통한 중앙 집권적으로 조직을 통제하는 것이 가장 쉬은 기술적인 측면 중심으로 보안에 대해 접근하였고 이 방법이 가장 효과적이라고 말 할 수는 없다.[14]

2011년부터 3년간 우리나라 국민 4,399만 명의 의료정보 47억 건을 미국 기업이 약 20억 원에 불법적으로 사들인 후 가공하여 약 100여억 원에 제약업체에 판매 한 사건이 있었고[15], 2016년 민중 총궐기 집회에서 물 대포를 맞고 입원치료를 받다 숨진 고(故) 백남기씨의 전자의무기록(EMR)을 무단으로 열람한 서울대병원 의사와 간호사 135명이 처분을 받은 사건이 있었다[16].

또한, 최근에는 police.com인 메일주소로 경찰을 사칭해 발송된 '온라인 명예 훼손 관련 출석요구서'메일을 확인, 첨부된 출석요구서를 다운 받아 랜섬웨어에 걸리는 일이 의료계에 발생했다.[17]

이는 의료기관의 전형적인 정보 보호 방법인 보안시스템구축, 방화벽설치, 백신 등과 같은 기술적인 측면에 더 중점을 두어 증가하는 보안 위협을 관리하고 통제하기 위해서 바이러스 예방프로그램이나 침입 통제 같은 기술적 측면[18]에 집중한 결과로 보인다.

지금까지의 정보보호 활동이 정보침해 사고 예방에 대해 얼마만큼 효과적인지에 대한 상관관계를 정확하게 판단하기는 어려우나, 정보보호활동은 정보 자산에 대한 관리적 보안, 시스템 분야에 대한 기술 보안, 그리고 시설에 대한 접근 제한을 위한 물리적 보안 이외에도 정보보호에 대한 인식 전환을 동반한다.

왜냐하면 정보보호분야는 공격기술이 방어기술보다 더 뛰어난 측면으로 P2P, Phishing, 스파이웨어, 랜섬웨어 등 다양한 공격기술이 사회공학적 공격기법과 융합되어 정보보호 기술 및 솔루션으로는 한계가 있어 정보보호를 모든 참여자들이 생활화하기 위한 정보보호 인식 제고를 하여야 하며[19] 이는 정보보호 인식의 제고가 자산, 정책 및 정보보호 인식 교육이 자리 잡는 것으로 정보보호 관리 모델에서 볼 때 조직의 정보보호를 이끌어가는 가장 큰 축의 하나이기 때문이다

그러나, 한국정보보호진흥원(KISA, Korea Internetand Security Agency)이 2017년 기업별로 조사한 정보보호 실태조사('A Survey of Information Security)' 결과에 따르면 정보보호교육을 실시한 기업의 비율은 28.1% 불과하다.[20]

이에 본 연구는 의료기관에 대해 기술적 정보보호 조치는 법에 따라 수행하였다는 전제 하에 기술적 물리적 정보 보안 요인은 통제하고, 조직 구성원들의 정보 보호 인식 제고를 위한 정보보호 교육을 실시할 경우, 조직 구성원들의 정보보호 생활화 참여 정도를 실증하여 의료기관들의 정보보호교육을 촉진할 수 있는 근거를 마련하고자 한다.

Ⅱ. 연구방법

1. 연구자료

1) 자료원(Data source)

본 연구에서는 2017년 한국보건산업진흥원이 실시한 「2017년 보건의료정보화 현황조사」 자료를 2차 활용하여 분석을 실시하였다. 이 자료는 한국보건산업진흥원이 건강보험심사평가원의 2016년 12월 기준 의료기관전체 리스트 중 약국과 조산원을 제외한 의료기관을 전체 모집단으로 하여 상급종합병원과 종합병원은 전수 추출하고, 병원은 심사청구건수 기준으로 제곱근 비례 배분하고 종합병원 및 치과병원의 경우 표본설계과정에서 국군 및 경찰병원을 제외한 전체 규모를 반영하여 표본을 추출하였다. 의원은 진료과목별 지역별 의료기관규모를 고려하여 층화효과를 반영한 표본을 추출하여 표본규모를 2,000개

로 설계하고 의료기관 7,033개를 접촉하여 2,002개의 의료기관에서 조사를 성공(응답율 28.5%)한 자료를 그대로 사용하여 모집단을 적절하게 대표한다.

2) 독립변수 : 정보보호교육횟수

각 기관별로 직원들에게 실시하는 정보보호교육에 대한 교육 실시 횟수를 설정하였다. 조사된 원 자료에서는 각 의료기관내 교육 대상 직원을 7개 직종(경영진, 의료인, 약사 의료기사 등 진료지원부서인력, 행정직, 전산직, 용역직, 기타)으로 분류하고, 각 직종별 교육 실시 횟수를 교육을 한번도 안 한 경우, 한번만 한 경우, 두 번 이상으로 조사하여, 정보 보호 교육이 실시된 직종 중 교육 횟수가 최소인 값을 기관의 교육 횟수로 보정하였다.(모든 직종에서 교육을 받지 않은 경우, 교육을 한번도 안 한 경우로 보정)

3) 종속변수 : 정보보호실천항목갯수

각 의료기관에서 조직 구성원들이 실천하고 있는 정보보안 항목의 실천 개수를 설정하였다. 조사된 원 자료에서는 각 의료기관내에서 조직 구성원들이 실천하여야 할 정보 보안 항목을 아래와 같이 11개로 제시하고, 각각의 항목에 대해 실천여부를 조사하여, 본 연구에서는 실천한다고 답한 항목의 개수를 해당 의료기관의 정보 보안 실천 항목의 개수로 보정하여 사용하였다.

4) 보정변수

보정변수는 의료기관종별, 직종, 지역을 포함하였다. 의료기관변수는 종합병원(상급종합병원, 종합병원), 병원(병원, 한방병원, 치과병원), 의원(의원, 한의원, 치과의원)으로 구분하고 있으며, 직종은 경영진(병원 경영진, 의원은 의사), 의료인(병원 의사, 간호사, 임상병리사, 방사선사, 약사 등), 행정직(전산직을 제외)으로 구분하였고, 지역의 경우 metropolitan(서울), urban(부산, 인천, 대구, 광주, 대전, 울산, 세종), rural(도 지역)로 구분하였다.

2. 분석방법

이 연구는 의료기관 전체를 모집단으로 하여 추출한 표본 의료기관을 대상으로 의료기관 종사자별(경영진, 의료인, 행정직 등)로 실시된 정보보호교육횟수와 소속 직원의 정보화보안실천항목(11가지항목, 종속변수에서 기술)의 실천하고 있는 갯수를 조사하여, 정보보호교육횟수와 정보화보안실천항목실천갯수와의 관련성을 카이제곱 검정(chi-square test)을 통해 우선 확인하고, 다중 회귀분석(multiple regression analysis)을 사용해 다변량 분석을 실시하였고 추가적으로 의료기관 규모별 정보보호교육횟수와 정보보안생활실천개수를 다변량 로지스틱 회귀분석(multivariate logistic regression analysis)을 사용하여 분석하였다. 자료의 정리와 통계분석은 SAS9.4로 처리하였다.

〈2017년 보건의료정보화 현황 조사된 보안 실천 항목〉

① 컴퓨터 로그인 패스워드 설정
② 화면보호기 설정(10분 이내)
③ 안전한 비밀번호 작성 규칙의 수립, 적용(주기적 변경)
④ 윈도우 보안패치 자동 업데이트 설정
⑤ 바이러스 백신 및 스파이웨어 제거 프로그램 설정
⑥ 비 인가된 P2P, 웹하드, 공유 설정 등에 대한 접속차단 실시
⑦ 개인(의료)정보 파일 암호화 설정
⑧ 개인(의료)정보 파일 복제(USB, CD 등 저장매체) 및 이메일 전송 금지
⑨ 개인정보 파일 완전 삭제(휴지통 비우기 실시)
⑩ 개인정보가 포함된 서류, 보조저장 매체 등은 안전한 장소 보관(잠금장치 등)
⑪ 백신 소프트웨어 설치 및 정기적 업데이트

Ⅲ. 연구결과

1. 분석대상자의 일반적 특성

〈표 1〉은 분석에 사용된 일반적인 사항으로 275개 종합병원은 9.520개, 424개의 병원은 8.083개, 135개의 요양병원은 8.141개, 1,168개의 의원은 6.886개의 정보보안생활실천을 하여 의료기관종별 규모가 커짐에 따라 정보보안생활실천을 더 하는 것으로 나타났다.

기관의 정보보호교육횟수가 없는 경우는 6.590개의 정보보안생활실천을 하는 반면 1회 교육을 실시하면 7.648개, 2회 이상 교육을 실시하면 8.435개로 교육을 실시할수록 정보보안생활실천을 하는 것으로 나타났다.

또한 기관에서 직종별로 교육을 받는 것과 정보보안생활실천개수를 보면, 경영진은 교육을 받지 않았을 때 5.621개였던 반면 교육을 받으면 7.813개로, 의료진은 교육을 받지 않았을 때 5.520개가 교육을 받으면 7.755개로, 행정직은 교육을 받지 않았을 때 5.367개가 교육을 받으면 8.133개로 모든 직종에서 교육을 받는 경우 증가하는 것을 알 수 있다.

지역별로 분석한 결과는 특별시 7,587개, 광역시 7.642개, 도 지역 7.553개로 정보보안생활실천을 하였다.

〈표 2〉의 내용을 확인하면 의료기관은 80.1%(n=2,002, 1회교육 61.29%, 2회 이상 교육 18.83%)가 정보보호교육

<표 1> 일반적 특성 (Genderal charactrictics)

	Total		실천갯수		P-value
	N	%	Mean	SD	
의료기관종별	2,002	100.0			<.0001
(상급)종합병원	275	13.7	9.520	1.839	
병원	424	21.2	8.083	2.580	
요양병원	135	6.7	8.141	2.554	
의원	1,168	58.3	6.886	2.965	
지역별	2,002	100.0			0.145
특별시	407	20.3	7.587	2.951	
광역시	581	29.0	7.642	2.876	
도지역	1,014	50.7	7.553	2.860	
기관의정보보호교육최소횟수	2,002	100.0			<.0001
교육안함	398	19.9	6.590	2.957	
1회교육	1,227	61.3	7.648	2.814	
2회이상교육	377	18.8	8.435	2.715	
정보보호교육여부_경영진	2,002	100.0			0.000
교육안함	195	9.7	5.621	2.911	
교육함	1,778	88.8	7.813	2.797	
대상자없음	29	1.5	6.897	2.782	
정보보호교육여부_의료진	2,002	100.0			0.470
교육안함	150	7.5	5.520	2.724	
교육함	1,845	92.2	7.755	2.830	
대상자없음	7	0.4	7.286	3.200	
정보보호교육여부_행정직	2,002	100.0			0.041
교육안함	79	4.0	5.367	2.918	
교육함	1,281	64.0	8.133	2.686	
대상자없음	642	32.1	6.768	2.936	

을 실시하고 있는데, (상급)종합병원 76.73%(n=275, 1회교육 49.45%, 2회 이상 교육 27.27%), 병원81.13%(n=424, 1회 교육 61.79%, 2회 이상 교육 19.34%), 요양병원 91.11% (n=135, 1회 교육 66.67%, 2회 이상 교육 24.44%), 의원 79.28%(n=1,168, 1회교육 63.27%, 2회 이상 교육 16.01%)로 나타났다. 교육 실시 비율은 (상

<표 2> 의료기관 종별 정보보호교육횟수 현황 (Number of information protection education by medical institutions)

	Total		(상급)종합병원		병원		요양병원		의원		P-value
	N	%	N	%	N	%	N	%	N	%	
정보보호교육횟수	2002	100.0	275	100.0	424	100.0	135	100.0	1168	100.0	<.0001
교육안함	398	19.8	64	23.2	80	18.8	12	8.8	242	20.7	
1회교육	1227	61.2	136	49.4	262	61.7	90	66.6	739	63.2	
2회이상교육	377	18.8	75	27.2	82	19.3	33	24.4	187	16.0	

<표 3> 기관별정보보호교육과 정보보안생활실천갯수와의 연관성 (Adjusted effect between Information security education and Information Protection Practice)

	실천갯수			
	B	95% CI		P-value
의료기관종별				
(상급)종합병원	1.975	1.519	2.431	<.0001
병원	0.841	0.484	1.198	<.0001
요양병원	0.827	0.317	1.337	0.002
의원(=ref)				
지역별				
특별시	0.337	0.029	0.645	0.032
광역시	0.058	-0.212	0.329	0.672
도지역(=ref)				
기관의정보보호교육최소횟수				
교육안함(=ref)				
1회교육	0.527	0.108	0.945	0.014
2회이상교육	1.067	0.597	1.536	<.0001
정보보호교육여부_경영진				
교육안함(=ref)				
교육함	0.806	0.201	1.411	0.009
대상자없음	-0.335	-1.472	0.802	0.564
정보보호교육여부_의료진				
교육안함(=ref)				
교육함	0.093	-0.567	0.753	0.783
대상자없음	0.717	-1.326	2.759	0.492
정보보호교육여부_행정직				
교육안함(=ref)				
교육함	0.765	0.018	1.512	0.045
대상자없음	0.413	-0.295	1.120	0.253

AIC (smaller is better) : 9609.8068

급)종합병원보다 의원, 병원, 요양병원순으로 높게 나타났으나, 2회 이상 교육으로 확인하면 의원, 병원, 요양병원, (상급)종합병원순으로 나타나고 있다.

의료기관의 정보보호교육 실시 비중을 한국인터넷진흥원이 조사한 2017년 정보보호실태조사[20]에서 실시한 산업별 개인정보보호 교육 실시 비율과 비교하면 금융 및 보험업의 교육 실시율 91.0% 보다는 낮은 수준이나, 정보서비스업(54.4%), 기술서비스업(30.9%) 등 보다 높은 수준이다. 다만, 250인 이상의 대규모 사업체의 정보 교육 실시 비율인 89.2%보다는 낮은 수준임을 알 수 있다.

2. 의료기관의 정보보호교육횟수와 정보보안 생활 실천 갯수와의 연관성

의료기관에서 실시되는 정보보호교육횟수와 정보보안 생활실천갯수의 회귀분석결과, 교육을 받지 않은 경우에 비해 교육을 1회 받은 경우 0.527개(B: 0.525, 95% CI[confidence interval]: 0.108-0.945, p: 0.014)높았고, 였고 교육을 2회 이상 받은 경우 1.067개(B: 1.067,95% CI: 0.597-1.536, p: <.0001) 높았다.

의료기관 규모별은 분석한 결과는 의원에 비해 (상급)종합병원은 1.975개(B: 1.975, 95% CI: 1.519-2.431, p: <.0001), 병원 0.841개(B: 0.841, 95%CI: 0.484-1.198, p: <.0001), 요양병원 0.827개(B: 0.827, 95%CI: 0.317-1.337, p: 0.002) 증가하였다. 의료기관 지역별은 도 지역에 비해 특별시 0.337개(B: 0.337, 95% CI: 0.029-0.645, p: 0.032), 광역시 0.058개(B: 0.058, 95%CI: -0.212-0.329, p: 0.672)로 나타났다.

또한, 의료기관 내 직종별(경영진,의료진,행정직)로 실시된 정보보호교육이 직원들의 정보보호 활동에 영향을 미치는지를 확인한 결과, 정보보호교육을 경영진이 받은 경우, 안 받을 경우에 비해 0.806개(B: 0.806, 95%CI:

<표 4> 기관별정보보호교육과 정보보안생활실천갯수와의 연관성 (Adjusted effect between Information security education and Information Protection Practice)

(병원급이상(Hospital Level), n=834)

	실천갯수			
	B	95% CI		P-value
지역별				
특별시	0.57	0.07	1.07	0.02
광역시	0.02	-0.34	0.37	0.93
도지역(ref)				
기관별정보보호교육횟수				
교육안함(ref)				
1회교육	0.09	-0.36	0.55	0.69
2회이상교육	0.65	0.12	1.17	0.02
정보보호교육여부_경영진				
교육안함(ref)				
교육함	0.78	-0.40	1.95	0.20
대상자없음	-0.25	-1.74	1.24	0.74
정보보호교육여부_의료진				
교육안함(ref)				
교육함	0.58	-2.13	3.29	0.67
대상자없음				
정보보호교육여부_행정직				
교육안함(ref)				
교육함	0.22	-3.65	4.10	0.91
대상자없음	-2.94	-6.74	0.85	0.13

<표 5> 기관별정보보호교육과 정보보안생활실천갯수와의 연관성 (Adjusted effect between Information security education and Information Protection Practice)

(의원급(Clinic Level),, n=1,168)

	실천갯수			
	B	95% CI		P-value
지역별				
특별시	0.31	-0.09	0.71	0.13
광역시	-0.02	-0.42	0.38	0.93
도지역(ref)				
기관별정보보호교육횟수				
교육안함(ref)				
1회교육	1.06	0.26	1.86	0.01
2회이상교육	1.81	0.93	2.69	<.0001
정보보호교육여부_경영진				
교육안함(ref)				
교육함	0.60	-0.24	1.43	0.16
대상자없음				
정보보호교육여부_의료진				
교육안함(ref)				
교육함	-0.22	-1.01	0.56	0.57
대상자없음	0.40	-1.83	2.62	0.73
정보보호교육여부_행정직				
교육안함(ref)				
교육함	0.66	-0.17	1.50	0.12
대상자없음	0.31	-0.49	1.11	0.45

0.201-1.411, p: 0.009)로 높았고, 안 받은 경우 대비 의료진이 교육을 받으면 0.093개(B: 0.093, 95%CI: -0.567-0.753, p: 0.783), 행정직은 0.765개(B: 0.093, 95%CI: 0.018-1.152, p: 0.045)로 나타났으며 모형적합도 결과 AIC(Akaike's Information Criterion)는 9609.8로 나타났다.〈표 3〉

의료기관종별을 (상급)종합병원, 병원, 요양병원을 묶어 분석한〈표 4〉를 보면 교육을 받지 않았을 때에 비해, 1회 교육시 0.09개, 2회 이상 교육시 0.65개가 증가하였고 경영진이 교육을 받은 경우 0.78개를 더 정보보안 생활 실천을 한 것으로 나타났다.

〈표 5〉와 같이 의원급은 교육을 받지 않은 경우에 비해, 교육을 1회 받으면 1.06개, 2회 이상 받으면 1.81개가 증가하는 것으로 나타났다. 또한, 경영진이 교육을 받는 경우 0.60개 더 증가하는 것으로 나타났다.

2013년 한국보건사회연구원의 '의료기관의 개인정보보호현황과 대책'[21]에 따르면 의원급의 의사들은 일반국민의 개인의무기록정보에 대한 관심수준을 5점 만점에 2.21점으로 평균(2.94점)보다 낮다고 생각하고, 의사의 관리 수준은 의원급 3.15점, 병원급은 3.33점으로 보통보다 높다고 생각하였으나,

최근 1년 동안 개인정보 보호관련 교육 경험률은 8.5%로 매우 낮았으며, 교육을 받지 않은 이유는 충분한 정보 및 소개가 부족하여 45.8%, 시간을 내지 못하여 19.8%, 필요성을 못 느껴 18.8%, 적절한 교육내용을 찾지 못하여 15.6% 순으로 나타났었는데 본 연구에서 나타난 결과는 의원급 의사들(경영진)의 생각과는 다르게 의원급 경영진(의사)은 정보보호교육을 받아야 정보보호를 위한 생활 실천을 한다는 것이 증명되었고, 정보보호를 자율적으로 의료기관에 맡기는 것 보다는 적절한 제3자 개입이 필요하다는 선행연구의 타당성이 증명되었다.[22]

Ⅳ. 고찰 및 결론

의료정보 관련 정보시스템의 발전은 의료서비스 종사자 및 환자에게 많은 편리함이 있지만, 이와 비례하여 개인정보의 유출은 재산상의 손실, 사회적 평가 저하 등의 불이익 뿐만아니라 신체에 대한 위해를 받을 수 있는 가능성은 증가하고 있다.

정보의 훼손, 변조, 유출 등을 방지하기 위해 정보시스템과 인터넷과의 분리, 침입차단시스템과 같은 보안 장비 도입 등의 물리적, 기술적 방법 뿐만아니라 개인 정보 유출, 남용 방지[23] 등을 위해 정보를 안전하게 보호 및 운영 할 수 있도록 개인정보의 접근 권한, 개인정보의 수집 범위, 자료공유의 범위[24] 등 관리적 관점에서의 보안이 요구 되고 있다.

정부는 2012년 3월 「개인정보보호법」시행을 통해 개인정보의 생성 수집부터 파기까지 개인정보를 취급하는 전 과정에 대한 구체적이고 체계적인 관리 기준을 규정하고, 「개인정보보호법」에 따라 고시된 '개인정보의 안전성 확보 조치'기준[25]을 지원하기 위해 '개인정보보호 자율규제단체 지정 등에 관한 규정(행정자치부 고시 제2016-31호, 2016.8.9. 제정)'을 시행하고 있다.

의료분야에서 자율규제단체로는 대한병원협회, 대한의사협회, 대한치과의사협회, 대한한의사협회, 대한약사회로 단체 소속 기관들과 개인정보보호자율규제규약을 맺고 이를 근거로 해당 기관들에 대한 자율점검 및 현장지원 등의 활동을 하고 있으며, 이는 규모가 작은 의료기관을 포함하여 개인정보보호교육을 실시하는 의료기관의 평균이 80.1%로 나타난 다양한 원인 중 한가지로 추정한다.

아울러, 일부 의료기관과는 아직 자율규제규약을 맺고 있지 않은 점은 보완해 나가야 할 것이며, 자율점검의 영향이 개인정보보호에 어떠한 영향을 미치는지에 대한 분석이 향후 이루어질 필요성이 있다.

또한, 기관이 정보보호교육을 받으면 정보보호생활실천이 높아지는 연구 결과와 기관에서 근무하는 근무자 직종별로도 정보보호교육을 받으면 정보보호생활실천이 높아진다는 결과에도 불구하고, 교육 대상에 대해서는 추가적인 검토가 필요하다.

예를 들어 의원 홈페이지 관리 형태는 위탁관리 53.8%, 자체와 위탁 병행이 19.2%, 자체관리 26.9%라는 조사결과는 외부인력의 환자개인정보에 대한 접근성이 높다는 것[21]을 시사하며 외부 인력에 대한 정보보호교육의 필요성을 반증하는 것으로 정보보호교육계획 수립 시 외부 인력에 대한 교육 방안을 마련할 것을 제언하는 바이다.

이에 따라, 조직에 근무하는 모든 구성원들이 조직의 보안을 위해 지켜야만 하는 많은 정보보호 수칙들을 각자의 위치에서 모두가 잘 지킬 수 있도록[19] 효과적인 보안 정책을 세우고 이를 구성원들이 실행할 수 있도록[26] 정보보호에 대한 교육이 필요하다.

이 연구의 목적은 의료기관에서 구성원에 대한 정보보호교육이 정보보호 활동을 증가시킨다는 실증을 통해, 의료기관에서 정보보호교육을 활성화할 수 있는 근거를 마련하고자 하였다. 이 연구의 주요 결과는 다음과 같다.

첫째, 의료기관의 정보보호교육횟수와 정보보호활동의 상관관계를 확인한 결과, 의료기관에서 정보보호교육을 받으면 조직구성원들의 정보보호활동의 참여가 증가하는 것을 알 수 있었다. 정보보안담당자들은 가장 큰 정보보호의 위협이 되는 사람은 보안 위협이 미흡하거나 조심성이 없는 직원들로 조직 내부의 상황을 가장 잘 알고 권한 있는 내부자에 의한 보안이 취약해 지는 상황을 만든다는 응답[27]과 기업이 조직 구성원의 행동을 보안 교육을 통해 적절하게 통제하게 된다면 기술적인 접근보다 훨씬 효과적일 수도 있다는 기존 연구[28]와도 일치한다.

둘째, 정보보호교육의 횟수가 증가하면 할수록 조직구성원들의 정보보호활동 참여가 늘어난다는 것을 알 수 있었다. 회사에서 실시하는 정보보호에 관련된 교육은 직원들의 인식에 직접적인 효과가 있다는 것이다. 평소 보안에 신경을 쓰지 않다가 교육의 기회를 통해 보안에 관련된 인지도가 향상되고 중요성을 깨닫게 된다는 선행 연구[29]의 내용을 확인할 수 있다.

셋째, 의료기관 경영자들에게 정보보호교육을 실시할 경우, 조직구성원들의 정보보호활동의 참여가 증가하는 것을 알 수 있었다. 이는 정보보호에 대한 최고경영층의 리더십이 높은 조직은 그렇지 않은 조직에 비해 정보보호 교육 및 훈련, 정보보호 정책수립활동이 큰 차이가 있고[30] 공공기관에서 최고경영층의 지원이 정보보호 거버넌스에 크게 영향을 미치고 정보보호에 있어서 가장 중요한 요인임을 확인[31]하고 조직의 정보보호 수준 향상에 가장 중요한 요인의 최고경영자의 정보보호에 대한 지원[32] 및 최고경영자의 정보보호에 대한 조직적 차원의 지원은 정보보호 성숙도 수준에 긍정적인 영향[33]을 준다

는 기존 연구 결과와도 유사한 결과를 얻었다.

마지막으로 의원급에는 정보보호교육이 필요하다는 점이다. 의사들의 개인정보보호 관리수준에 대한 5점 만점에 본인 의원에서의 개인의무기록정보 보호 관리수준을 질문하면 3.38점으로 나타나지만 평균은 3.15점으로 나타나 인식의 차이를 보인 점[21] 등과 의원급에서 정보보호교육에 따른 정보보호실천갯수가 증가가 나타난 점을 고려할 때 소규모 기관들을 교육할 수 있는 방안을 마련할 필요가 있음을 확인되었다.

본 연구는 지금까지의 연구들에서 대표성을 갖는 전국단위의 의료기관을 대상으로 정보보호교육횟수와 조직 구성원들의 정보보호 활동과의 연관성을 실증하였다는데 의의가 있으며, 이러한 결과는 의료기관은 경영진을 비롯해 의료기관 종사자에 대한 정보 보호 교육을 실시하여야 한다는 당위성 제공에 근거로 활용될 수 있을 것이다. 아울러, 의료기관에 대한 개인의료정보보호에 대한 관리 실태 및 인식 수준을 주기적으로 파악할 수 있는 조사가 없는 실정으로 주기적인 실태조사를 통해 문제점을 파악하고 현실적 대책을 마련할 필요가 있다고 하겠다.

다만, 본 연구는 첫째, 이 연구는 우리나라의 의료기관 정보화 현황을 파악하고, 이에 대한 효과적인 정책수립의 기초자료를 확보하기 위한 목적으로 조사된 한국보건산업진흥원의 「2017년 보건의료정보화 현황조사」 자료를 2차 활용한 것으로 원자료의 조사 목적에 따른 바이어스가 있을 수 있으며, 둘째, 표본 추출을 통해 조사된 자료로 특정의료기관과는 다른 결과가 나타날 수 있고, 셋째 기관의 사용자 개개인의 생활실천개수를 조사한 것이 아니라, 기관 단위로 조사하였기 때문에 자료가 가지고 있는 특성으로 인한 바이어스가 있을 수 있으며, 넷째 설문에 의존하였기 때문에 답변자에 따른 바이어스가 있을 수 있다는 조사자료의 제한점과

병원의 규모가 커질수록 정보보호실천갯수가 증가하는 연구 결과는 종업원 1000명 이상 기업은 72.3%가 정보보호교육을 실시했다고 한 반면 300명 미만의 기업은 27.6%에 불과하여 기업간 격차가 크다는 선행 발표와 동일한 반면,[34] (상급)종합병원이 교육을 하지 않은 기관의 비율이 23.27%로 가장 많았음에도 정보보호생활실천갯수가 가장 많이 나타난 이유는 다른 요인이 작용한 것으로 보인다는 점,

종단 연구가 아닌 횡단면 연구로 인하여 의료기관의 정보 보안 교육의 변화에 따른 구성원들의 정보보호생활 참여 정도와의 상관 관계 분석에 한계가 있는 점

통제된 정보 보호 거버넌스, 정보 보호를 위한 장비 및 솔루션 등 조직 구성원의 정보보호 생활 참여에 영향을 줄 수 있다는 점 등을 고려할 때, 추가적인 연구가 필요할 것으로 판단된다.

<참고문헌(Reference)>

[1] Lee, H.J., The Legislation on the Personal Medical Information Protection Law. Korean Journal of Medicine and Law 2014. 22(1): p. 177-208.

[2] Jeong, G.W., Use and protection of medical information. Journal of Korea Association For Informedia Law, 2002. 6(1): p. 3-4.

[3] Jang, S.C., The Lgislation on the Protection of Medical Information. The Journal of Law, 2013. 24(2): p. 425-446.

[4] Jeong, B.G., Issues on the Patient's Information Protection. THE KOREAN SOCIETY OF LAW AND MEDICINE, 2008. 9(2): p. 339-382.

[5] Lee, H.J., The Legislation on the Personal Medical Information Protection Law. Korean Journal of Medicine and Law, 2014. 22(1): p. 177-208.

[6] Cho, H.S., Protection of Individual Medical Information in Risksociety. Hanyang law review, 2013. 24(4): p. 171-191.

[7] Park, J.H., Impact of Personal Health Information Security Awareness on Convenience. The Journal of the Korea Contents Association, 2017. 17(6): p. 600-612.

[8] Baek, Y.C., Medical Service Information and Individual Information Protection in Korea. Constitutional Law, 2005. 11(1): p. 395-442.

[9] Care at a hospital medical institution Personal information protection. boannews, 2013. 6. 27.

[10] Jeong, H.J., Kim, N.H., A Study on the institution of a Personal Health Information Protection Law - With the focus on the Personal Information Control Right -. The Journal of

Korea Association of Medical Law, 2008. 16(2): p. 99-121.

[11] Von Solms, B., Information security-the fourth wave. Computers & security, 2006. 25(3): p. 165-168.

[12] Wei, H., Frincke, D., Carter, O., and Ritter, C., Cost-benefit analysis for network intrusion detection systems. CSI 28th Annual Computer Security Conference, October, Washington DC, USA,, 2001: p. 29-31.

[13] Aron, J.L., Gove, R. A., Azadegan, S., and Schneider, M. C., The Benefits of a Notification Process in Addressing the Worsening Computer Virus Problem : Results of a Survey and a Simulation Model. Computers and Security, 2001. 20(8): p. 693-714.

[14] Dhillon, G.a.J.B., Information System Security Management in the New Millennium. Communications if the ACM, 2000. 43: p. 125-128.

[15] Kim, H.N., In the era of personal information leakage, protection of personal medical information. Research Institute for Healthcare Policy Korea Medical Association, 2014. 12(1): p. 71-77.

[16] Confession to leave EMR unauthorized visit Seoul National Univ. Medical Today News, 2019.1.21.

[17] "Online Defamation Attendance" Medical Ransomware Red Alarm. MedicalTimes, 2019-02-26.

[18] GoodHue, D.L.a.D.W.S., Security Concerns if System Users: A Study of Perceptions of the Adequacy of Security Measures. Information & Management, 1991. 20: p. 13-27.

[19] Lim, C.H., Effective information protection awareness improvement plan. Journal of the Korea Institute of Information Security, 2006. 16(2): p. 30-36.

[20] Agency, K.I.S., 2017 Survey on Information Security Businiess. Korea Internet & Security Agency, 2017.

[21] Jung, Y.C., Lee, K.H., Lee, Y.R., A Study on Current Privacy Policies of Medical Institutes and Suggestions. Korea Institute for Health and Social Affairs, 2013. 29.

[22] Lee, C.S., Information security auditing framework in industrial control system. Journal of the Korea Institute of Information Security & Cryptology, 2008. 18(1): p. 139-148.

[23] Moon, K.W., Kim, S.G., Relationship between Information Security Activities of Enterprise and Its Infringement : Mainly on the Effects of Information Security Awareness. Journal of the Korea Institute of Information Security & Cryptology, 2017. 27(4): p. 897-912.

[24] Chu, J.H., Wang, S.H., Cho, Y.W., Park, M., Lee, B.R., A Study on the Improvement of Legal System for Activation of Medical Information Industry. Korea Information Society Development Institute, 2003: p. 99-100.

[25] Ministry of Public Administration and Security, Notice No. 2017-1(2017.7.26).

[26] Amitava, D.a.K.M., Manangement's Role in Information Security in a Cyber Economy. California Management Review, 2002. 45: p. 67-87.

[27] Choi, D.K., Song, M.S. , Im, J.I. , Lee, K.H., Study the role of information security personnel have on an organization's information security level. Journal of The Korea Institute of Information Security & Cryptology, 2015. 25(1): p. 197-209.

[28] Straub, D.W., Effective IS Security: An Empirical Study. Information Systems Research, 1990. 1: p. 255-276.

[29] Park, J.K., Kim, B.S., Cho, S.W. , Primary Factors Affecting Corporate Employees' Attitudes Toward Information Security. Korea Business Review, 2011. 40(4): p. 955-985.

[30] Yoo, J.H., Comparison of Information Security Controls by Leadership of Top Management. Journal of Korea Society of Electronic Commerce, 2014. 19(1): p. 63-78.

[31] Song, J.S., Jeon, M. J., and Choi, M. G., A Study on Factors Affecting the Level of

Information Security Governance in Korea Government Institutions and Agencies. The Journal of Society for e-Business Studies, 2011. 16(1): p. 133-151.

[32] Joshi, K., The measurement of fairness or equity perceptions of management information systems users. MIS Quarterly, 1989. 13: p. 343-358.

[33] Choi, M.G., An Exploring Study on Relation Between Maturity Levels of Organizations and Factors Affecting Information Security Policy. Journal of Korean Academic Association of Business Administration, 2009. 22(3): p. 1729-1748.

[34] Lee, G.G., [Future society hopes for technology] 〈Part 3〉 We need social security strategy. Naeilnews, 2009.11.15.