요양기관 개인정보보호 자율점검에 관한 연구
A Study On Privacy Check Of Medical Institutions

이야리(개인정보통합관제센터)
박홍민(건강보험심사평가원)

차 례

■ keyword : | Privacy Protection | Privacy Self-Check | Medical Information Protection | Personal Information Leakage|

1. 서론

개인정보보호법 시행('11.09) 이후에도 개인정보 유출 사고가 적지 않고 사태의 심각성 또한 증대하다. 대표적 사고로는 '14년 카드사 개인정보 대량유출 1억여건(KB 국민카드 약 4,300만건, NH농협카드 약 2,200만건, 롯데카드 약 2,000만건), '15년 지누스社 병원 진료기록 유출(7억건에 달하는 진료기록을 무단으로 빼돌려 한국IMS헬스社에 판매) 등 개인정보 유출사례가 지속적 발생해 왔으며 정보의 특성상 유출될 경우 심각한 사회적 파장이 예상되는 의료정보의 유출은 국민의 불안감을 크게 유발할 수 있다.

개인정보보호법을 주관하는 행정자치부(이하 '행자부')는 개인정보보호 관리를 위해 매년 공공기관에 대한 점검을 실시하고 민간에 대해서도 정기/수시점검의 형태로 개인정보보호 수준관리 강화를 위해 실태점검을 통해 현황 파악 및 결과에 따라 조치 등을 이행함으로써 개선을 유도하고 있다. 그러나 모든 국민을 대상으로 점검을 실시하는 것은 수행 기간과 수반되는 인력, 예산 차원의 효율성, 효과성을 쉽게 예상할 수 없다. 따라서 개인정보처리자들(기관)이 자율 점검을 할 수 있도록 사업자 협회나 단체 같은 기구가 자율규제 활동을 이끌어 가도록 권장하고 있다. 이는 「개인정보보호법」 제13조의 자율규제의 촉진 및 지원을 위해 필요한 시책 마련이라는 취지와도 부합하는 것이다[1].

본 연구에서는 국민의 의료정보를 처리하는 국내 요양기관의 개인정보보호 자율점검 서비스 및 활동에 대한 현황, 개선점을 제시하였다.

2. 배경연구

2.1 요양기관 개인정보보호 자율점검

개인정보보호법은 공공과 민간 분야 모두 준수해야하는 것으로 법 의무 조치사항 준수에 대한 감독을 행정기관에서만 수행하기엔 한계가 있다.

개인정보 유출사고 중에서도 의료 정보가 포함된 개인정보 유출은 매우 중대한 사안으로 행자부와 보건복지부(이하 '복지부)는 의료기관의 개인정보 보호를 위해 '요양기관 개인정보보호 자율점검' 실시를 통해 자발적인 개인정보보호 체계 마련을 권장하였다. 요양기관의 개인정보보호 자율점검 수행기관은 보건복지부 산하기관인 건강보험심사평가원(이하 '심평원)이다.

'요양기관 개인정보보호 자율점검'이란 민감한 개인정보를 처리하는 요양기관을 대상으로 개인정보 관리 실태를 점검하고 개인정보보호법에 위배되는 부분에 대해 스스로 보완해나갈 수 있도록 유도하는 제도이다. 자율점검 대상은 보건 기관 및 조산소를 제외한 약 8만 4천 여개의 병·의원 및 한의원, 약국 등 대부분의 요양기관이 해당된다 [2].

만약 자율점검에 참여하지 않을 경우 현장점검의 대상이 되며, 이때 개인정보 유출 등 개인정보보호법 위반 사항이 적발될 경우 행정 처분으로 이어질 수 있다.

2.2 의료정보 관련 법령 동향[3]

의료정보를 기록하는 전자의무기록에 대한 관련 법령 근거는 다음과 같다.

복지부 보건의료정책과-3385(5.11) 『전자의무기록의 적법한 전자서명에 대한 안내』에 따르면 의료법 제23조에서 규정하는 전자의무기록상 전자서명 진료기록부에 의료인이 해야 하는 서명의 효과를 갖추기 위해서는 전자서명법상의 공인전자서명이어야 한다. 최근 판례에서 의료인이 전자문서(EMR) 진료기록 작성시 전자서명법에 의한 전자서명을 해야만 전자의무기록으로 본다(서울행정법원 2014구합64865관련)고 결정되었다. 따라서 전자의무기록에 공인전자서명을 하지 않을시 자격정지 15일 및 300만원 이하의 벌금을 물어야 한다.

의료법 제22조(진료기록부)에서 “의료인은 진료기록부에 의료행위 관한 사항과 의견을 상세히 기록하고 서명하여야 한다.” 또한 제23조(전자의무기록)에서는 “의료인이나 의료기관 개설자는 진료기록부등을 전자서명법에 따른 전자서명이 기재 된 전자문서로 작성·보관할 수 있다.”고 하였다.

전자서명법 제2조(정의)에서 전자서명이란 “서명 자료를 확인하고 서명자가 당해 전자문서에 서명을 하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부하거나 논리적으로 결합된 전자적 형태의 정보를 말한다.”, 공인전자서명의 정의는 “공인인증서를 기초한 전자서명을 말하며, 전자서명 및 전자문서의 변경여부 확인이 가능” 해야 한다고 되어 있다.

표 1. 의료 관련 법령 등의 개정

구문	조문내용	공통조치사항	외부보관 시 요구 사항
제1호 제2호	· 전자 의무기록(EMR) 생성 및 전자서명 검증	· 전자의무기록 생성 및 전자서명 · 전자의무기록 이력관리	
제3호	· 백업저장 장비	· 주기적 백업 · 잠금장치가 구비된 보관장소	· 무중단 백업 및 긴급 복구 · 백업데이터에 대한 위변조 탐지 · 백업설비의 분리운영
제4호 제5호	· N/W보안 및 전자 의무기록 시스템 보안	· 접근 통제 및 권한 제한 · 개인정보의 (전송)암호화 · 접속기록의 보관 · 보안프로그램 설치	· N/W 이중화 · 인증된 보호제품 사용 · 데이터 무결성 보장 · 접근통제 시스템 구성 · 데이터 관리방안
제6호	· 물리적 접근방지 시설	· 보관시설 마련 · 잠금장치 설치 등	· 출입통제구역 설치 · 출입통제 및 모니터링 · 장비 소재지를 국내로 제한
제7호	· 외부보관 시 필요시설 및 장비 또는 백업장비를설치하는 경우		· 실시간 모니터링 · 장애대비 예비 장비 운영 · CCTV설치·운영 · 침입감지 장비운영 · 재해예방시설 설치 등

표 1은 최근 개정된 의료법 시행규칙 제16조 제1항(전자의무기록을 안전하게 관리·보존 및 외부저장)과 고시(시설 장비·세부기준)에서 규정하는 전자의무기록 및 시설장비에 대한 규정을 법 조문, 공통적 조치사항, 외부보관에 대한 요구사항으로 정리한 것이다.

3. 요양기관 개인정보보호 자율점검 서비스

3.1 자율점검 서비스 개요

요양기관 개인정보보호 자율점검 서비스는 “자율점검 서비스”와 “자가점검 서비스”로 구성된다.

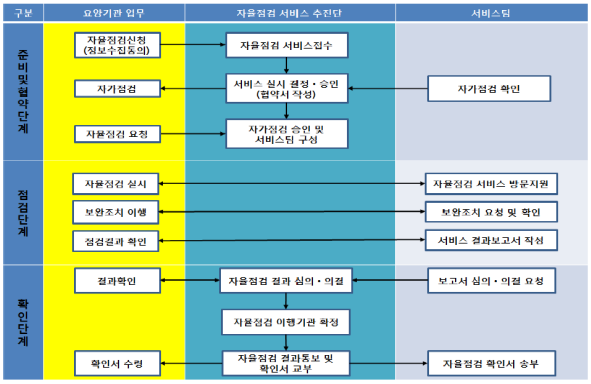
본 서비스의 목적은 요양기관 스스로 개인정보보호법 규정을 이해하고 준수 할 수 있도록 하면서, 각 기관의 개인정보 관리 실태를 자율적으로 파악하여 미비한 사항에 대하여 스스로 보완하는데 도움을 주는 용도이다.

그림 1에서 자율점검 서비스 수행은 신청한 기관이 점검 대상의 범위를 결정하고 의약단체(대한의사협회, 대한병원협회, 대한치과의사협회, 대한한의사협회, 대한약사회)와 심평원의 협업을 통해 자율적 점검을 진행하게 된다. 또한 요양기관 정보화지원 협의회는 요양기관업무포털시스템을 통해 ‘요양기관 개인정보보호 자가점검 서비스(’16.6.1 개시)’를 제공한다[3].

심평원 본원과 지원은 전국 권역별로 신청 요양기관에 대한 서비스 이행과 교육을 통해 지속적으로 서비스에 대한 지원을 수행함으로써 민간의료기관에 대한 개인정보보호 수준의 상승효과와 영속성 유지를 궁극적 목표로 하고 있다.

▶▶ 그림 1. 개인정보보호 자율점검 서비스 개념도

개인정보보호 자율점검 서비스는 크게 3단계(준비・협약단계, 점검단계, 확인단계)로 구분되고 수행 기관별로 요양기관, 자율점검 서비스 추진단(이하 '추진단'), 서비스팀에서 각 단계별 업무를 수행한다[4]. 개략적으로 설명하면 요양기관의 자율점검 신청을 시작으로 추진단에서는 서비스 실시를 결정하며 요양기관의 자율점검 요청에 따라 서비스팀에서는 해당 요양기관을 방문하여 자율점검 보완조치 이행 확인 및 지원을 하고 결과보고서를 작성하여 추진단에 심의・의결 단계를 거친다. 최종적으로 추진단은 결과 통보 및 확인서를 교부하게 된다[그림 2. 참고].

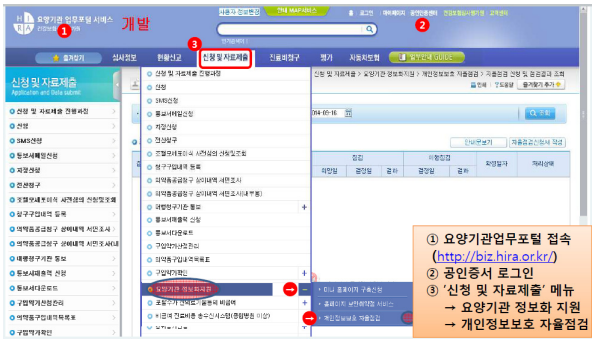


▶▶ 그림 2. 개인정보보호 자율점검 서비스 흐름도

3.2 자율점검 지원 시스템(Self Check Support System)

요양기관 개인정보보호 자율점검 서비스는 요양기관업무포털(http://biz.hira.or.kr/)에 접속하여 자율점검 지원 시스템(이하 'SCSS')을 통해 이루어진다[5]. SCSS는 서비스 신청 5단계, 자율점검 승인, 자가점검 실시, 자율점검 내역 등록 및 최종 제출, 점검 처리 상태 확인, 자율점검 결과 조회 등의 기능 및 관련 프로세스를 실행한다(그림 3.~6. 참고).

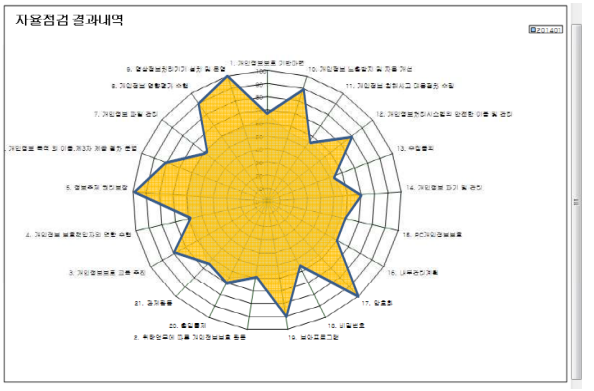
본 자율점검 서비스 수행을 위한 체크리스트는 개인정보 보호법 준수사항 이행 및 관리수준 점검을 위해 3개 분야(개인정보의 처리/개인정보의 처리제한/개인정보의 안전한 관리), 18개 영역, 25개 항목(표2. 참고)으로 나뉘어 있다. 세부 항목은 요양기관에 따라 다소의 차이가 있는데, 병원 59개, 치과 및 한의원 55개, 약국은 44개 항목이다. 그리고 약국에 대해서는 최근 유형별・조건별로 점검 항목이 달라져 5인 미만의 소형 약국은 23개 항목을 점검하면 된다.



▶▶ 그림 3. SCSS : 자율점검 신청 단계 예시

▶▶ 그림 4. SCSS : 자율점검 승인 및 자가점검 실시 단계 예시

▶▶ 그림 5. SCSS : 자율점검 승인 및 자가점검 실시 단계 예시



▶▶ 그림 6. SCSS : 자율점검 승인 및 자가점검 실시 단계 예시

표 2. 요양기관 개인정보보호 자율점검표 예시(출처: 요양기관 개인정보보호 자율점검 서비스 교육자료)

분야	영역	법근거	점검항목
1. 개인정보 처리(수집·이용·제공)	개인정보의 수집·이용	제15조	온·오프라인 회원 가입 시 동의 받고 있는가?
			각종 게시판, 기타 개인정보 수집 시 동의 받고 있는가?
	개인정보의 수집제한	제16조	목적에 필요한 최소한의 개인정보 수집하고 있는가?
	개인정보의 제공	제17조(18조)	제3자에게 개인정보 제공 및 목적 외 이용 시 정보주체의 별도 동의는 받고 있는가?
	개인정보의 이용·제공제한	제18조	개인정보 제공 시 제공 목적범위 내 이용, 안전조치 실시, 목적 달성 후 파기 등을 요청하고 있는가?
	개인정보의 파기	제21조	보유기관 경과, 처리목적 (제공받은 경우 제공받은 목적) 달성 후 지체 없이 개인정보는 파기하고 관리대장을 작성하여 관리하고 있는가?
	동의를 받는 방법	제22조	만14세 미만 아동의 개인정보를 수집하는 경우 법정대리인의 동의를 받고 있는가?
			홍보 권유에 활용하기 위한 정보와 그렇지 않은 정보를 구분하여 동의를 받고 있는가?
2. 개인정보 처리 제한	민감정보의 처리제한	제24조	고유식별정보의 수집 및 제공 시 개인정보 수집 동의와 별도로 구분하여 동의 받는가?
	영상정보처리기기의 설치·운영 제한	제25조	영상정보처리기기 운영·관리방침을 수립하고 있는가?
			영상정보처리기기를 설치한 장소에 정보주체가 인지할 수 있도록 필수 기재사항을 포함한 안내판을 설치하였는가?
			개인영상정보에 대한 이용·제공·열람·파기 내역을 기록관리하는가?
	업무위탁에 따른 개인정보의 처리제한	제26조	위탁계약 시 문서(계약서)에 의한 계약을 하였는가?
	개인정보 취급자에 대한 감독	제28조	개인정보취급자에 대한 보안 서약서는 징구하였는가?
			개인정보취급자 및 일반직원에 대한 정기적인 교육은 실시하였는가?
3. 개인정보의 안전한 관리	내부관리 계획수립	제29조 안전조치 의무	내부관리계획을 수립하고 필수사항을 포함하고 있는가?
	접근권한 관리 및 접근통제		안전한 비밀번호 작성규칙을 적용하고 있는가?
	개인정보 암호화		개인정보 암호화계획을 수립하여 시행하고 있는가?
	접속기록 보관		취급자의 접속기록을 최소 6개월 이상 보관하여 관리하고 있는가?
	보안 프로그램 설치·운영		개인정보처리시스템에 백신프로그램 등 최신의 보안 프로그램을 설치하여 관리하고 있는가?
			보안프로그램을 정기적(일1회이상)으로 업데이트 하는가?
	물리적 접근방지		전산실, 자료보관실 등 물리적 보관 장소에 대한 출입통제절차를 수립·운영하고 있는가?
	개인정보 처리방침 수립 및 공개	제30조	개인정보 처리방침을 홈페이지 등에 공개하고 있는가?
	개인정보 보호책임자 지정	제31조	개인정보보호책임자가 지정되고 그 역할이 정의되어 있는가?

3.3 자율점검 현황

요양기관 개인정보보호 자율점검 서비스 대상은 의료법 및 약사법에 따라 개설된 의료기관 및 약국 등 총 86,269개 기관(2016년 5. 50 기준 (보건기관 제외))이고 그동안의 주요 추진경과를 살펴보면 다음과 같다[3].

- 2014년 5월 : "요양기관 정보화 지원 협의회" 워크숍에서 서비스 모델 협의
- 2014년 12월 : 자율점검서비스 시범 실시(2개 기관)
- 2015년 4월 : 자율점검서비스 시스템 개발, 자율점검 추진단 구성 및 점검 실시
- 2015년 8월 : 전체 의료기관 및 약국 대상 자가점검 서비스 확대
- 2015년 12월 : 의료기관 및 약국 대상 자율점검 서비스 종료
- 2016년 5월 : 2015년도 개인정보보호 자가점검 서비스 종료
- 2016년 4월 : 2016년도 개인정보보호 자율(자가)점검 서비스 실시

표 3은 자율점검서비스의 추진 실적 현황으로 자가점검 대상 총 86,269개 기관 중에서 참여기관 수는 75,002개(약 87%)이고 그 중 점검을 완료한 곳은 70,821개 기관(약 94%)이다.

표 3. 요양기관 종별 자가점검 서비스 추진 실적

종별	전체기관 수	신청기관		자가점검기관			
		기관 수	비율	완료	비율	미완료	비율
합계	86,269	75,002	86.9%	70,821	94.4%	4,181	5.6%
상급병원	43	32	74.4%	31	96.9%	1	3.1%
종합병원	294	249	84.7%	237	95.2%	12	4.8%
병원	1,510	1,222	80.9%	1,132	92.6%	90	7.4%
요양병원	1,397	1,185	84.8%	1,132	95.5%	53	4.5%
의원	30,039	25,324	84.3%	24,035	94.9%	1,289	5.1%
치과병원	217	179	82.5%	171	95.5%	8	4.5%
치과의원	16,779	13,992	83.4%	13,230	94.6%	762	5.4%
약국	21,967	20,567	93.6%	19,244	93.6%	1,323	6.4%
한방병원	262	217	82.8%	194	89.4%	23	10.6%
한의원	13,761	12,035	87.5%	11,415	94.8%	620	5.2%

교육 및 홍보활동을 위해 전국 주요 도시 22개 지역을 대상으로 약 22,929개의 기관 교육 및 강사 지원을 실시하였다.

2016년 자율점검 서비스는 4월부터 11월까지 온라인 자가점검 및 현장지원을 수행할 예정이며 점검결과에 대한 분석 및 피드백은 10월에서 12월까지 완료될 것이다.

4. 결론

요양기관 개인정보보호 자율점검 서비스는 2014년 시범운영을 시작으로 2016년 8월 현재 계속 진행 중이며

지금까지의 경과는 상당한 개선 효과를 보이고 있다. 그러나 자율점검 서비스는 용어 그대로 자율적 측면을 강조한 것으로써 법에 의한 행자부의 현장점검 및 행정처분에 영향을 주는 법적 효력은 없다고 할 수 있다. 다만, 의료기관이 현장 점검에 대한 사전 대비이며 조치 미흡에 따른 요양기관의 피해를 최소화하고자 하는 궁극의 목표에 부합한 것일 뿐이다. 따라서 요양기관에서는 본 자율점검 서비스에서 제공하는 관련 법 시행규칙 및 고시 등의 변화 등에 따른 점검사항 등을 꾸준히 모니터링하여 자체적으로 개선하여야 하고 보건의료 관련 분야의 특화된 내용을 참조하여 의료기관이 관련 법적 요구사항 미비로 인하여 불이익을 받는 일이 없도록 하고, 정보주체인 환자(국민)가 개인정보에 관해 안심하고 진료를 받을 수 있도록 노력해야 한다. 또한 심평원 및 협·단체에서는 요양기관들이 자율점검 서비스를 이용함에 있어 최소한의 노력으로 최대 효과를 얻을 수 있도록 체계적으로 시스템 등을 개선해야 할 것이다. 예를 들어 담당자들이 시스템을 통해 자가점검을 신청할 경우 입력해야 하는 항목의 간소화, 서비스화면의 편리성, 직관성, 가독성 강화, 점검기준의 제시 기능 추가 등이 필요할 것이다.

본 논문에서는 국내 요양기관의 개인정보보호 자율점검 활동과 현황을 파악하였다. 결과적으로 개인정보처리자인 요양기관에서는 환자정보 유출 예방 및 법적 의무사항을 준수하기 위해 자율·자가 점검을 지속적으로 수행하고 관련 협의체와도 유기적인 서비스 활동을 도모하여 의료서비스 수준향상이라는 궁극의 목표를 위해 노력해야 할 것으로 기대한다.

참고문헌

[1] 2015 개인정보보호연차보고서, 행정자치부, 2015년

[2] AhnLab '개인정보보호 자율점검', http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=24336, 2015년 11월

[3] 국내 의료기관의 개인정보보호 자율점검 활동, ISACA Korea Conference, 2016년 9월

[4] 요양기관 개인정보보호 자율점검 서비스, 건강보험심사평가원, 2015년

[5] 자가점검 서비스 사용법(업무포털), 건강보험심사평가원, 2015년

저자소개

● 이 야 리(Ya Ri Lee)

- 1990년 2월 : 고려대학교 전자전산공학과(공학사)
- 1999년 2월 : 동국대학교 교육대학원(컴퓨터교육학석사)
- 2002년 8월 : 동국대학교 컴퓨터공학과(공학박사)
- 2001년 ~ 2012년 : 삼육보건대학교 겸임교수 등 역임
- 2012년 ~ 현재 : 개인정보통합관제센터 팀장

<관심분야> : 개인정보보호, 빅데이터, 클라우드컴퓨팅, IoT 보안 등

● 박 홍 민(Hong Min Park)

- 현재 : 건강보험심사평가원 정보통신실 과장

<관심분야> : 개인정보보호, 보건의료분야 (개인)정보보호 자율점검 활동 및 보건의료분야 빅데이터 등 컨텐츠 저작권 관리 관련 등