우리나라 의료기관의 개인정보 보호 인증제도 적용을 위한 정책과제[1)]

A Study on Personal Information Protection Certification of Medical institutions in Korea

정영철 한국보건사회연구원 연구위원
이야리 한국보건사회연구원 초빙연구위원

대부분 의료기관에서 생산, 보관, 관리되고 있는 환자의 질병 및 치료정보와 같은 개인의료정보는 매우 민감하고도 중요하여 정보보호가 시급히 필요한 바, 기존의 홈페이지 인증, 정보보호 관리체계 인증, 개인정보보호 관리체계 인증 등과 같은 자율규제적 인증제도를 비교 · 검토하여 도입할 필요가 있다. 이에 본 고에서는 개인의료정보보호 인식 및 환경 제고측면에서 첫째, 의료기관의 개인정보보호 관리현황에 대한 주기적인 실태파악, 의료기관 종류별 맞춤형 필수 관리지침 개발 및 보급, 의료기관별 맞춤형 컨설팅 및 교육 제공, 보건복지분야 개인정보보호 전문기관 육성 등과 같은 준비과제를 제안하고자 한다.

1. 서론

산업사회에 이어 정보와 지식이 경제활동의 중심이 되고 국가 경쟁력의 원천이 되는 '정보화사회'에서 정보화, 정보통신기술은 인간 삶의 더할나위 없는 편리하고도 필요한 기능이며 도구인 동시에 불법스팸, 해킹, 프라이버시침해, 개인정보 오남용 등과 같은 역기능을 초래하기도 한다.

그 중에서도 개인정보에 대한 의도적인 혹은 의도치 않은 유 · 노출과 오남용은 개인, 사회, 국가에 대한 상당한 피해를 발생시켜 많은 국가들이 국가적 차원에서 법제화를 추진하고 민간차원의 자율규제를 수행하는 등 개인정보 보호를 위한 보다 적극적인 노력을 기울이고 있다. 특히 환자의 질병 및 치료정보와 같은 개인의료정보는 대부분 의료기관에서 생산, 보관, 관리되고 있으며 정보특성상 가장 민감하고도 보호가 필요한 정보로 국가차원의 종합적이고도 체계적인 노력과 대책이 요구된다 하겠다.

이에 대해 우리나라에서는 개인정보 보호를 위한 법제화 측면에서는 1994년 통신비밀보호법을 시작으로 관련 법률들이 제정되었고[2)] 2011년 3월 마침내 공공과 민간, 사회 전 영역을 아우르는 「개인정보 보호법」이 제정, 같은 해 9월부터 시행되고 있으며 민간차원의 자율

1) 본 원고의 내용은, 한국보건사회연구원의 2013년도 기본과제인 "의료기관의 개인정보 보호현황과 대책" 연구 수행의 일환으로 작성되었음.
2) 정혜영(2011). **개인정보 보호법의 내용과 체계에 관한 분석**, 공법학연구, 12(4), pp.407~435, 한국비교공법학회.

규제 측면에서는 인증제를 도입하여 시행하고 있다.

한편, 우리나라 의료기관에서의 개인정보 보호 관리체계[3]는 전체적으로 미흡하여 공공이나 금융부문과 같은 타 산업분야에 비해 개인정보 보호 수준제고가 절실히 요구되고, 개인정보 보호법 이후에도 이행정도가 저조하게 나타나[4] 의료기관에서의 개인정보 보호수준 제고를 위한 방법 중 하나로 자율규제 성격인 인증제 도입에서 그 대안을 찾고자 한다. 이를 위해 본 고에서는 우리나라의 개인정보 보호관련 각종 인증제도와 더불어 우리나라 개인정보 보호법 체계와 매우 비슷한 일본의 개인정보 보호 인증제도인 프라이버시 마크제도를 분석 · 비교하여 의료기관에서의 개인정보 보호 수준향상을 위한 인증제 적용에 있어 그 준비과제를 모색해보고자 한다.

2. 개인정보 유출 및 개인정보 보호

'개인정보'란 살아있는 한 개인에 관한 정보로, 그 정보로 해당 개인을 알아볼 수 있는 정보를 뜻하며(개인정보 보호법 제2조) 일반정보, 가족정보, 병역정보, 소득정보, 신용정보, 의료정보, 위치정보 등으로 구분하기도 한다(표 1 참조). 그 중에서도 개인의 의료정보, 즉 '개인의료정보'는 개인의 질병정보, 검사정보, 진단정보, 건강보험정보, 사망기록정보 등[5] 개인의 민감한 정보로써, 손실 혹은 파손이 발생하면

표 1. 개인정보의 종류

구분	항목
일반정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년월일, 출생지, 본적지, 성별, 국적
가족정보	가족구성원들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술자격증 및 전문면허증, 이수한 훈련프로그램, 동아리활동, 상벌사항
병역정보	군번 및 계급, 제대유형, 주특기, 근무부대
부동산정보	소유주택, 토지, 자동차, 기타소유차량, 상점 및 건물 등
소득정보	현재 봉급액, 봉급경력, 보너스 및 수수료, 기타소득의 원천, 이자소득, 사업소득
기타 수익정보	보험 (건강, 생명 등) 가입현황, 회사의 판공비, 투자프로그램, 퇴직프로그램, 휴가, 병가
신용정보	대부잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 임금압류 통보에 대한 기록

3) 기업이 전사차원에서 개인정보보호 활동을 체계적 · 지속적으로 수행하기 위해 필요한 일련의 보호조치 체계를 말하며, 기업이 개인정보보호를 위해 무엇을(what to do), 어떻게(how to do) 조치하여야 하는지에 대한 기준을 제시한다(개인정보보호 종합지원포털 중 '용어사전', http://www.privacy.go.kr/nns/ntc/wor/WordDicaryListInqire.do, [인용 2013.10.30.]).

4) 김동수 · 김민수(2006). **e-Health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향,** 정보화정책, 13(4), pp.128~148, 서울: 한국정보화진흥원; 조혜경(2008). **의료기관의 개인건강정보 보호 실태와 관리방안,** 충남대학교 대학원 박사학위논문; 엄현호(2013). **의료기관의 개인정보 보호법 이행현황 및 개선방안에 관한 연구,** 가톨릭대학교 보건대학원 석사학위논문; 데일리메디(2013.07.18.), http://dailymedi.com/news/view.html?section=1&category=4&no=769424.

〈표 1〉 계속

구분	항목
고용정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트결과 직무태도
법적정보	전과기록, 자동차 교통 위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물테스트 등 각종 신체테스트 정보
조직정보	노조가입, 종교단체가입, 정당가입, 클럽회원
통신정보	전자우편(E-mail), 전화통화내용, 로그파일(Log file), 쿠키(Cookies)
위치정보	GPS나 휴대폰에 의한 개인의 위치정보
신체정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가활동, 비디오 대여기록, 도박성향

자료: 개인정보보호 종합지원 포털 중 '안내광장', http://www.privacy.go.kr/nns/ntc/inf/personalInfo.do, [인용 2013.10.30.].

환자안전에 심각한 영향을 끼칠 뿐 아니라 유 · 노출에 의해 환자와 가족, 친지에 이르기까지 심각한 후유증에 시달릴 수도 있으며 해당 의료기관 평판에도 상당한 부정적 영향을 끼치게 된다.

이러한 개인정보가 전자매체에 대량으로 수집 · 축적되고, 이용 · 관리되면서 개인정보 유노출사고가 빈번하게 발생하였으며(표 2 참조) 개인정보 유 · 노출에 대한 위험성, 개인정보 보호에 대한 중요성과 필요성은 점점 확대되고 있다.

이와 같이 정보주체의 개인정보에 대해 개인정보처리자가 법령이나 개인정보처리자의 의사에 의하지 않고, 통제를 상실하거나 권한 없는 자의 접근을 허용하는 것을 '개인정보 유출'이라 하고(표준 개인정보 보호지침 제26조) 이를 막기 위해 개인정보 관리체계 수립, 개인정보 처리단계별 기준 · 절차 준수 및 안전한 관리, 정보주체 권리보장 등을 지속적으로 수행하는 일련의 조치와 활동을 '개인정보 보호'라 한다(개인정보 보호 인증제 운영에 관한 규정 제2조). '개인정보 보호'는 타인에 의한 개인정보 수집 · 처리와 관련하여 해당 개인정보 주체의

표 2. 국내 주요 개인정보 유출사고 현황

시기	업체	피해규모
2006~2008	하나로텔레콤	650만명
2008년 2월	옥션	1,863만명
2008년 9월	GS칼텍스	1,119만명
2010년 3월	신세계몰	330만명
2011년 4월	현대 캐피탈	175만명
2011년 7월	SK커뮤니테이션즈	3,500만명
2011년 11월	넥슨	1,320만명
2012년 4월	EBS	400만명
2012년 7월	KT	870만명

자료: 아주경제(2013.09.23), http://www.ajunews.com/kor/view.jsp?newsId=20130922000122#.

5) 백윤철(2005). **헌법상 환자의 의료정보에 대한 권리에 관한 연구**, 헌법학 연구, 11(3), pp.337~373.

이익을 나타내는 개념이다[6].

한편 개인의료정보는 주로 의료기관에서 생산 · 이용 · 관리되고 있는 바, 의료기관의 많은 업무 정보화로 대규모 디지털화가 이루어지고, 인터넷 및 웹환경이 확대되며, e-Health, u-Health, smart-Health와 같은 IT기술발전에 의한 의료환경변화는 개인의료정보 유노출 위험을 더욱 더 증가시키고 있다[7].

실제로 미국에서는 2009년 이후부터 서터메디컬재단 및 서터피지션 서비스 이용 고객의 환자 의료정보 유출을 포함해 미국 내에서 약 600여건의 유출사건이 일어나 2,200만명의 피해자가 발생하였다고 하며[8] 우리나라에서도 의료기관 내부직원의 관리소홀 및 의도적인 유출로 인해, 그리고 외부 관리업체 직원의 의도적인 유출 및 외부 해킹에 의해 개인의료정보 유노출 사건이 지속적으로 발생되고 있다(표 3 참조).

표 3. 2005년 이후 언론기사화된 우리나라 의료기관에서의 개인의료정보 유노출현황

번호	날짜	내용	출처
1	2006.10.03	부산 모 대학병원에서 내부직원에 의해 사망한 환자 주민등록번호 유출(대포폰 유통)	부산일보
2	2006.10.24	20여개 병원에서 환자 개인정보를 유출해 신용정보업체에서 채권추심에 사용	mbc
3	2007.10.11	전주 모병원에서 내부직원에 의해 환자개인정보가 무단유출되어 선거인단에 불법 등록	경향신문
4	2007.10.12	익산의 한 병원 간호조무사와 컴퓨터 수리업자 등에 의한 병원 9,800여명의 환자개인정보 무단 유출	국민일보
5	2009.05.19	한 유명연예인에 대한 진료기록 일부 유출	노컷뉴스
6	2010.02.03	국군대구병원에서 신검정밀의뢰서로 사용한 용지 이면지에서 개인의료정보 유출	경향신문
7	2011.05.04	전직 대통령의 X-선 사진 무단유출	데일리메디
8	2011.09.29	8개 대형병원에서 본인동의 없이 22만 여명의 환자 개인정보를 보건의료연구원에 불법 제공(국감)	보안뉴스
9	2012.03.13	서울시장 아들의 의료정보 무단유출	뉴데일리
10	2012.04.18	고물상에 병원처방전 폐지처분	C뉴스 041
11	2012.08.20	국립의료기관에서 환자 민감정보가 담긴 병력지를 이면지로 사용	노컷뉴스
12	2012.09.28	600여개 산부인과에서 의료기기 판매대행 업체에 환자개인정보 23만건 유출	조선일보
13	2012.10.31	구글검색으로 A산부인과 홈페이지에서 회원개인정보 17여만건 무단 유출	한국일보
14	2013.08.07	S통신사 전자차트(청구소프트웨어프로그램) 설치 의료기관에서 환자동의없이 개인정보 제3자 제공	청년의사
15	2013.10.02	해킹에 의한 국내 성형외과의 환자 개인정보 유출	JTBC TV

6) 이인호(2005). **개인정보 보호법의 합리적인 입법기준의 모색**, 디지털 정보의 효율적 이용과 프라이버시의 효과적 보호에 관한 정책토론회.

7) 이유지(2005). **병원보안 이슈와 과제**, 컴퓨터월드 7월호, pp.71~82, 서울: 아이티엠지; 한국정보보호진흥원(2006). **지식정보사회 의료 패러다임 변화와 정보보안**.

8) 보안뉴스(2013.06.27), http://www.boannews.com/media/view.asp?idx=36636&kind=1.

3. 국내 개인정보 보호관련 인증제도

앞에서 살펴본 개인정보 유노출 등을 막기 위한 자율규제성격의 '개인정보 보호 인증[9]' 제도로써 국내에서는 기업 및 기관의 홈페이지에 대한 개인정보보호 안전성을 확보하기 위한 인증제도와 기관 및 기업의 총체적인 개인정보보호 관리체계 확보를 위한 인증제도로 나누어질 수 있다. 먼저 인터넷사이트의 개인정보보호 안전성을 확보하기 위해 민간이 자율적으로 추진하고 있는 가장 대표적인 인증제도로는 '개인정보보호마크(*e*PRIVACY Mark)' 제도와 '인터넷사이트 안전마크(i-Safe Mark)' 제도 2가지가 있다. 다음으로 기관의 전반적인 개인정보보호 관리수준향상을 위한 인증제도에는 '정보보호 관리체계 인증(ISMS)', '개인정보보호 관리체계 인증(PIMS, Personal Information Management System)', 그리고 올해 말부터 인증심사 신청이 가능한 '개인정보 보호수준 인증(PIPL, Personal Information Protection Level)' 제도 등이 있다.

1) 홈페이지 개인정보 보호 인증제도

홈페이지에 대한 개인정보보호수준을 인증하는 개인정보보호 마크로는 '*e*PRIVACY(개인정보보호우수사이트마크)', 'i-Safe(인터넷사이트안전마크)' 2가지가 있다. 이들은 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'과 '개인정보 보호법'에 근거하여 기관 및 기업의 홈페이지 개인정보 보호수준을 심사하여 부여하는 민간자율적 인증마크제도로, 개인정보보호협회(OPA, Online Privacy Association) 정보보호마크 인증위원회가 주관하고 있다. *e*PRIVACY 마크는 2000년부터 시행되어 <표 4>와 같이 생명주기, 관리과정, 보호대책 등 3개 분야 총 86개 점검항목[10]을 기준으로 심사하며 i-Safe 마크는 2002년부터 시행되어 생명주기, 관리과정, 보호대책, 정보보호대책, 소비자보호 등 5개분야 총 136개 점검항목[11]을 기준으로 심사하고 있다[12].

*e*PRIVACY 마크와 i-Safe 마크 유효기간은 1년이며 2013년 10월 현재, *e*PRIVACY 마크가 유효하게 부여되어 있는 사이트는 138개, i-Safe 마크가 유효하게 부여되어 있는 사이트는 58개, 두 개 마크가 동시에 유효하게 부여되어 있는 사이트는 39개로 총 157개 사이트에 대해 *e*PRIVACY 마크 혹은 i-Safe 마크가 유효하게 부여되어 있었으나(표 5 참조) 의료기관의 경우 서울대학교병원 1개소만 홈페이지 개인정보보호 인증마크가 부여되어 있었다[13].

9) 기관의 개인정보 보호를 위한 일련의 조치와 활동이 특정 기준에 부합됨을 승인하는 것임(개인정보 보호 인증제 운영에 관한 규정 제2조).
10) 공공기관의 경우 98개 항목
11) 공공기관의 경우 122개 항목
12) 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20].
13) 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20].

표 4. 국내 홈페이지 개인정보보호인증마크 심사기준

구분	분야	영역	통제 항목수	세부 통제 항목수	점검 항목수
ePIVACY	생명주기	1. 개인정보 수집	4(4)	6(6)	13(15)
		2. 개인정보 수집의 특별조치	2(2)	2(2)	4(4)
		3. 개인정보의 이용	4(4)	5(6)	11(14)
		4. 개인정보의 파기	2(2)	3(3)	7(8)
	관리과정	1. 이용자의 권리	2(2)	4(4)	10(11)
		2. 공개 및 책임	3(3)	3(3)	9(9)
		3. 주민등록번호(고유식별번호) 처리	1(1)	2(2)	4(4)
	보호대책	1. 개인정보의 안전성 확보를 위한 기술적, 관리적 보호조치	5(7)	11(12)	25(29)
		2. 개인정보의 안전성 확보를 위한 물리적 보호 조치	2(2)	2(2)	3(4)
	합계		25(27)	38(40)	86(98)
iISafe	생명주기	1. 개인정보 수집	2(3)	4(4)	7(6)
		2. 개인정보 수집의 특별조치	1(1)	1(1)	2(2)
		3. 개인정보의 이용	4(3)	5(5)	11(11)
		4. 개인정보의 파기	2(1)	3(1)	7(3)
	관리과정	1. 이용자의 권리	2(2)	3(2)	8(6)
		2. 공개 및 책임	3(3)	3(3)	7(7)
		3. 주민등록번호(고유식별번호) 처리	0(1)	0(1)	0(3)
	보호대책	1. 개인정보의 안전성확보를 위한 기술적, 관리적 보호조치	2(3)	3(4)	7(10)
	정보보호대책(시스템보호)	1. 보완과 신뢰성 확보를 위한 물리적 요건	6(6)	7(7)	12(12)
		2. 보완과 신뢰성 확보를 위한 기술적 요건	10(10)	11(11)	21(21)
		3. 보완과 신뢰성 확보를 위한 관리적 요건	9(9)	16(6)	41(41)
	소비자보호	1. 소비자보호	2(0)	5(0)	13(0)
	합계		43(41)	61(44)	136(122)

주: 민간기업 심사기준. 단, ( )항목은 공공기관 심사기준
자료: 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20].

2) 정보보호 관리체계 인증제도 (ISMS, Information Security Management System)

ISMS 인증제도는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조(정보보호 관리체계의 인증), 그리고 동법 시행령 제47조(정보보호 관리체계 인증의 방법 · 절차 · 범위 등)에 근거하여 정보통신망의 안정성, 신뢰성 확보를 위해 관리적 · 기술적 · 물리적 보호조치를 포함한 종합적 관리체계를 수립 · 운영하고 있는 자에 대해 '정보보호 관리체계 인증 등에 관한 고시(미래창조과학부고시 제2013-36호)'에 따른 기준의 적합성을 인증하는 제도이다.

표 5. 국내 홈페이지 개인정보보호인증마크 부여(유효) 현황(2013년 10월현재)

구분	사이트 수	로고
ePRIVACY 유효	138	
i-Safe 유효	58	
ePRIVACY와 i-Safe 동시 유효	39	

자료: 개인정보보호인증마크제도 사이트, www.eprivacy.or.kr, [인용 2013.10.20].

본 제도는 미래창조과학부 주관 하에 한국인터넷진흥원이 인증기관으로서 인증에 관한 업무를 수행하며 학계 및 연구기관등 전문가로 구성된 인증위원회에서 인증심사결과를 심의·의결한다. 2013년부터는 의무적으로 인증을 받아야 하는 기업을 지정하고 있으며 의료기관은 의무인증대상기관에 해당되지는 않으나 중요자산 취급분야 중 하나로 자율적인 신청이 가능한 분야라 할 수 있다[14].

ISMS 인증에 대한 기준은 '정보보호관리' 분야와 '정보보호대책' 분야 등 크게 2개 분야로 나누어지며 '정보보호관리' 분야에 대한 요구항목으로는 정보보호정책수립 및 범위설정, 경영진 책임 및 조직구성, 위험관리, 정보보호대책 구현, 사후관리 등 5개 관리과정에 대해 12개 세부 관리과정으로 나누어 심사를 받게 된다. 다음으로 '정보보호대책' 분야에 있어서는 정보보호정책, 정보보호조직, 외부자 보안, 정보자산분류, 정보보호교육, 인적보안, 물리적 보안, 시스템 개발 보안, 암호통제, 접근통제, 운영보안, 침해사고관리, IT 재해복구 등 13개 영역, 총 104개 점검항목으로 구분하여 심사를 수행하고 있다(표 6 참조)[15].

이러한 ISMS 인증 취득에 대한 혜택으로는 가산점부여, 정보보호관련 보험가입시 할인 등이 있으며 ISMS 인증을 독려하기 위해 원격교육설비기준 및 유비쿼터스도시기반시설에 ISMS 인증 취득을 권고하고 일부 수수료 할인 제도도 마련하고 있다(표 7 참조)[16].

인증에 대한 유효기간은 3년이며, 2002년이후 2013년 10월 현재까지 발급된 ISMS 인증서는 총 170건으로 현재 유효한 인증기관은 133개소, 그 중 의료기관은 한군데도 없다[17].

14) 정보보호 및 개인정보보호관리체계 인증 사이트, http://isms.kisa.or.kr/, [인용 2013.10.20.].
15) 정보보호 관리체계 인증 등에 관한 고시(미래창조과학부 고시 제2013-36호).
16) 정보보호 및 개인정보보호관리체계 인증 사이트, http://isms.kisa.or.kr/, [인용 2013.10.20].
17) 정보보호 및 개인정보보호관리체계 인증 사이트, http://isms.kisa.or.kr/, [인용 2013.10.20].

표 6. ISMS 인증 심사기준

분야	관리과정		세부관리과정		
정보보호 관리	1	정보보호정책수립 및 범위설정	1.1	정보보호정책 수립	
			1.2	범위설정	
	2	경영진 책임 및 조직구성	2.1	경영진 참여	
			2.2	정보보호 조직 구성 및 자원 할당	
	3	위험관리	3.1	위험관리 방법 및 계획 수립	
			3.2	위험식별 및 평가	
			3.3	정보보호대책 선정 및 이행계획 수립	
	4	정보보호대책 구현	4.1	정보보호대책의 효과적 구현	
			4.2	내부 공유 및 교육	
	5	사후관리	5.1	법적요구사항 준수검토	
			5.2	정보보호 관리체계 운영현황 관리	
			5.3	내부감사	
통제분야			**통제목적**		**점검항목수**
정보보호 대책	1	정보보호정책	1.1	정책 승인 및 공표	2
			1.2	정책의 체계	2
			1.3	정책의 유지관리	2
	2	정보보호조직	2.1	조직의 체계	3
			2.2	역할 및 책임	1
	3	외부자보안	3.1	보안 요구사항 정의	1
			3.2	외부자 보안 이행	2
	4	정보자산분류	4.1	정보자산 식별 및 책임	2
			4.2	정보자산의 분류 및 취급	1
	5	정보보호교육	5.1	교육 프로그램 수립	3
			5.2	교육 시행 및 평가	1
	6	인적 보안	6.1	정보보호 책임	3
			6.2	인사규정	2
	7	물리적 보안	7.1	물리적 보호구역	5
			7.2	시스템보호	2
			7.3	사무실 보안	2
	8	시스템 개발보안	8.1	분석 및 설계 보안관리	4
			8.2	구현 및 이관 보안	5
			8.3	외주개발보안	1
	9	암호통제	9.1	암호 정책	1
			9.2	암호키관리	1

〈표 6〉 계속

통제분야			통제목적		점검항목수
정보보호 대책	10	접근통제	10.1	접근통제정책	1
			10.2	접근권한 관리	3
			10.3	사용자 인증 및 식별	4
			10.4	접근통제 영역	6
	11	운영보안	11.1	운영절차 및 변경관리	2
			11.2	시스템 및 서비스 운영보안	10
			11.3	전자거래 및 정보전송보안	2
			11.4	매체 보안	2
			11.5	악성코드관리	2
			11.6	로그관리 및 모니터링	4
	12	침해사고 관리	12.1	절차 및 체계	2
			12.2	대응 및 복구	3
			12.3	사후관리	2
	13	IT 재해복구	13.1	체계 구축	1
			13.2	대책 구현	2
로고					

자료: 정보보호 관리체계 인증 등에 관한 고시(미래창조과학부고시 제2013-36호).

표 7. ISMS 인증 취득의 혜택

구분	시행기관	혜택내용
가산점 부여	지식경제부	– 보안관제 전문업체 '업무수행능력 평가기준' 중 신뢰도 항목에 만점(5점) 부여 – 공공부문 정보시스템 기획 · 구축 · 운영 사업자, SW개발사업자 선정시 기밀보안 평가항목에 만점 부여
	KISA	– 정보보호대상, 입찰, 과제선정 평가시 가점 부여
	신용평가기관	– 한국신용평가정보의 기업신용평가 시 가점 부여
	한국기업지배구조원	– 상장기업 ESG(환경, 사회, 지배구조) 평가시 소비자항목에 가점 부여
요금할인	보험사	– 정보보호관련 보험(배상책임보험등) 가입시 할인
권고	교육과학기술부	– 원격교육설비기준에 인증취득 권고
	국토해양부	– 유비쿼터스 도시기반시설에 인증취득 권고
수수료 할인	KISA	– 정보보호 대상 수상기업의 경우 할인(대상, 우수상, 특별상: 100~50%) – 소규모기업의 경우 할인(상시 근로자 수 50명 미만 또는 매출액 50억 미만: 50%)

자료: 정보보호 및 개인정보보호관리체계 인증 사이트, http://isms.kisa.or.kr/, [인용 2013.10.20].

3) 개인정보보호관리체계 인증(PIMS, Personal Information Management System)

PIMS 인증제도는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제47조의3(개인정보보호 관리체계의 인증), 그리고 동법 시행령 제54조의2(개인정보보호 관리체계의 인증)에 근거하여 정보통신망에서 개인정보보호활동을 체계적이고 지속적으로 수행하기 위해 필요한 관리적, 기술적, 물리적 보호조치를 포함한 개인정보보호 관리체계를 수립 · 운영하고 있는 자에 대해 '개인정보보호 관리체계 인증 등에 관한 고시(방송통신위원회고시 제2013-17호)'에 따른 기준의 적합성을 인증하는 제도이다.

본 제도는 2010년부터 시행되었으며 방송통신위원회 주관 하에 한국인터넷진흥원이 인증기관으로서 인증에 관한 업무를 수행하며 정보보호전문가, 변호사, 교수 등 정보보호분야에 학식과 경험이 있는 자로 구성된 인증위원회에서 인증심사결과를 심의 · 의결한다.

이러한 PIMS 인증심사는 서면심사와 현장심사를 병행하며 인증기준은 개인정보보호를 체계적이고 주기적으로 수행하고 있는지를 점검하는 '개인정보보호 관리과정 분야' 13개항목, 개인정보를 안전하게 보호하기 위한 관리적, 물리적, 기술적 보호조치를 점검하는 '개인정보보호대책 분야' 80개항목, 개인정보 생성에서 파기까지의 법률준수 여부를 점검하는 '생명주기' 31개항목 등 크게 3개 분야로 나누어 총 124개 점검항목으로 구성하고 있다(표 8 참조)[18].

표 8. PIMS 인증 심사기준

분야	영역		통제목적		점검항목수
계					124
개인정보보호 관리과정	1	개인정보보호 정책수립 및 범위설정	1.1	개인정보보호정책 수립	1
			1.2	범위설정	1
			1.3	개인정보 흐름파악	1
	2	경영진 책임 및 조직구성	2.1	경영진 참여	1
			2.2	개인정보보호 조직 구성 및 자원 할당	1
	3	위험관리	3.1	위험관리 방법 및 계획 수립	1
			3.2	위험 식별 및 평가	1
			3.3	개인정보보호대책 선정 및 이행계획 수립	1
	4	개인정보보호 대책 구현	4.1	개인정보보호대책의 효과적 구현	1
			4.2	내부 공유 및 교육	1
	5	사후관리	5.1	법적 요구사항 준수검토	1
			5.2	개인정보보호 관리체계 운영현황 관리	1
			5.3	내부감사	1

18) 개인정보 보호 관리체계 인증 등에 관한 고시(방송통신위원회고시 제2013-17호)

〈표 8〉 계속

분야	영역		통제목적		점검항목수
보호대책	1	개인정보 보호정책	1.1	정책의 승인 및 공표	2
			1.2	정책의 체계	2
			1.3	정책의 유지관리	2
	2	개인정보 보호조직	2.1	조직체계	4
			2.2	역할 및 책임	2
	3	개인정보 자산분류	3.1	개인정보의 식별 및 책임	1
			3.2	개인정보의 분류 및 취급	1
	4	교육 프로그램 수립	4.1	교육계획	3
			4.2	교육 시행 및 평가	1
	5	인적보안	5.1	개인정보 취급자 관리	4
	6	침해사고관리	6.1	절차 및 체계	2
			6.2	대응 및 복구	3
			6.3	사후관리	2
	7	기술적 보호조치	7.1	접근통제	14
			7.2	암호통제	2
			7.3	운영통제	11
			7.4	매체보안	2
			7.5	시스템 개발보안	7
			7.6	접속기록 관리 및 모니터링	4
			7.7	출력, 복사 통제	1
			7.8	개인정보표시 제한	1
	8	물리적 보호조치	8.1	보호구역	5
			8.2	사무실보호	2
			8.3	영상정보처리기기 보안	1
생명주기	1	개인정보 수집에 따른 조치	1.1	최소한의 정보수집	5
			1.2	개인정보 수집시 고지 및 동의획득	3
			1.3	개인정보취급방침	1
	2	개인정보 이용 및 제공에 따른 조치	2.1	동의범위내 개인정보 사용	1
			2.2	이용자 권리보호	6
			2.3	외부 위탁시 개인정보 보호	4
			2.4	제3자 제공시 개인정보 보호	3
			2.5	개인정보 이전시 개인정보 보호	2
	3	개인정보 관리 및 파기에 따른 조치	3.1	개인정보 관리 및 파기	6
로고					

자료: 개인정보보호 관리체계 인증 등에 관한 고시(방송통신위원회 고시 제2013-17호).

PIMS인증에 대한 유효기간은 3년으로, 2011년이후 2013년 현재까지 PIMS 인증서는 총 29건이 발급되었다. 이러한 PIMS 인증 취득 시에는 해당 기업에서 개인정보 사고 발생시 과징금, 과태료를 경감해주는 인센티브를 부여하고 있으며 심사기준 변경부분에 대한 재인증심사 실시, 사후모니터링, 개인정보보호 우수성에 대한 홍보효과, 고가의 컨설팅 대비 비용절감, 개인정보보호관련 전문교육 기회획득, 정보보호 관련 수상에서의 가산점 획득, 템플릿 획득을 통한 개인정보관리계획 수립 용이 등과 같은 기대효과를 꾀하고 있다[19].

4) 개인정보 보호수준 인증제도(PIPL, Personal Information Protection Level)

PIPL 인증제도는 '개인정보 보호법' 제13조(자율규제의 촉진 및 지원)에서 규정하고 있는 '개인정보 보호 인증마크의 도입 · 시행 지원'에 의해 2013년 10월 '개인정보 보호 인증제 운영에 관한 규정(안전행정부 고시 제2013-45호)'이 제정 · 고시되었으며 PIPL 인증을 받고자 하는 기관은 2013년 11월 28일부터 인증심사를 신청할 수 있게 되었다.

본 제도는 안전행정부 주관 하에 한국정보화진흥원이 인증기관으로서 인증에 관한 업무를 수행하며 기업 및 기관의 개인정보 보호체계, 개인정보 보호활동 수준을 객관적으로 측정해 기관 규모와 특성에 따라 대기업 · 공공기관, 중소기업, 소상공인용 등 3개 유형으로 구분하여 인증하게 된다. 인증심사항목은 개인정보보호 관리체계 분야(15개 항목)와 개인정보 보호 대책구현 분야(50개 항목)로 나누어 총 65개 심사항목으로 구성되어 있으며 유효기간은 3년이다(표 9 참조)[20].

한편, PIPL 인증 취득 시 정부(안전행정부)는 '개인정보 보호법'에 따라 실시되는 기획점검 대상에서 제외 혹은 점검을 유예해주거나, 고의성 없는 위반사항에 대하여 과태료 등 행정처분 감경, 개인정보보호 교육기회 부여, 개인정보보호 우수기관에 대한 포상 실시 등과 같은 다양한 정책적 지원을 계획하고 있다[21].

4. 일본의 프라이버시 마크제도 (Privacy Mark)

다음으로 일본의 가장 대표적인 개인정보보호관련 인증제도로서 P 마크제도는 2005년 개인정보의 보호에 관한 법률(이하 개인정보 보호법)이 시행되기 이전인 1998년부터 민간자율규제적인 개인정보보호 인증제도로 도입하여 시행하고 있다.

일본의 프라이버시 마크(일명 P마크) 제도는 통산성(通産省) 산하 공공기관인 일본정보처리개 발 센 터 (JIPDEC: Japan Information Processing Development Center) 총괄 책임 하에 개인정보 보호에 대한 소비자들의 인식을 향상

19) 정보보호 및 개인정보보호관리체계 인증 사이트, http://isms.kisa.or.kr/, [인용 2013.10.20].
20) 개인정보 보호 인증제 운영에 관한 규정(안전행정부 고시 제2013-45조).
21) 안전행정부(2013.10.28.). **개인정보 보호법 준수기관, 인증받는다**, 안전행정부 보도자료.

표 9. PIPL 인증 심사기준

분야	영역		심사목적		심사항목수
개인정보보호 관리체계	1	보호체계의 수립	1.1	관리계획	2
			1.2	조직	1
			1.3	경영진의 책임	2
	2	실행 및 운영	2.1	문서화	1
			2.2	개인정보 식별	1
			2.3	위험관리	4
	3	검토 및 모니터링	3.1	개인정보보호체계의 검토및모니터링	2
	4	교정 및 개선	4.1	교정 및 개선활동 실적관리	1
			4.2	내부 공유 및 인식제고	1
개인정보보호 대책구현	1	개인정보 처리제한	1.1	개인정보 수집시 보호조치	7
			1.2	개인정보 이용 및 제공시 보호조치	3
			1.3	개인정보의 보유시 보호조치	2
			1.4	개인정보 파기시 보호조치	2
	2	정보주체 권리보장	2.1	권리보장	3
	3	관리적 안전성 확보조치	3.1	개인정보 보호책임자의 지정	1
			3.2	교육 및 훈련	2
			3.3	개인정보취급자 관리	2
			3.4	위탁업무관리	3
			3.5	개인정보 유출사고 대응	2
	4	기술적 안전성 확보조치	4.1	점근권한 관리	3
			4.2	접근기록 관리	2
			4.3	운영보안	7
			4.4	암호화 통제	2
			4.5	개발보안	2
	5	물리적 안전성 확보조치	5.1	영상정보처리기기 관리	2
			5.2	물리적 보안관리	5
로고					

인증2013-○○○○ 인증범위:_____	인증2013-○○○○ 인증범위:_____	인증2013-○○○○ 인증범위:_____	인증2013-○○○○ 인증범위:_____
〈유형3(공공기관용)〉	〈유형3(대기업용)〉	〈유형2(중소기업용)〉	〈유형1(소상공인용)〉

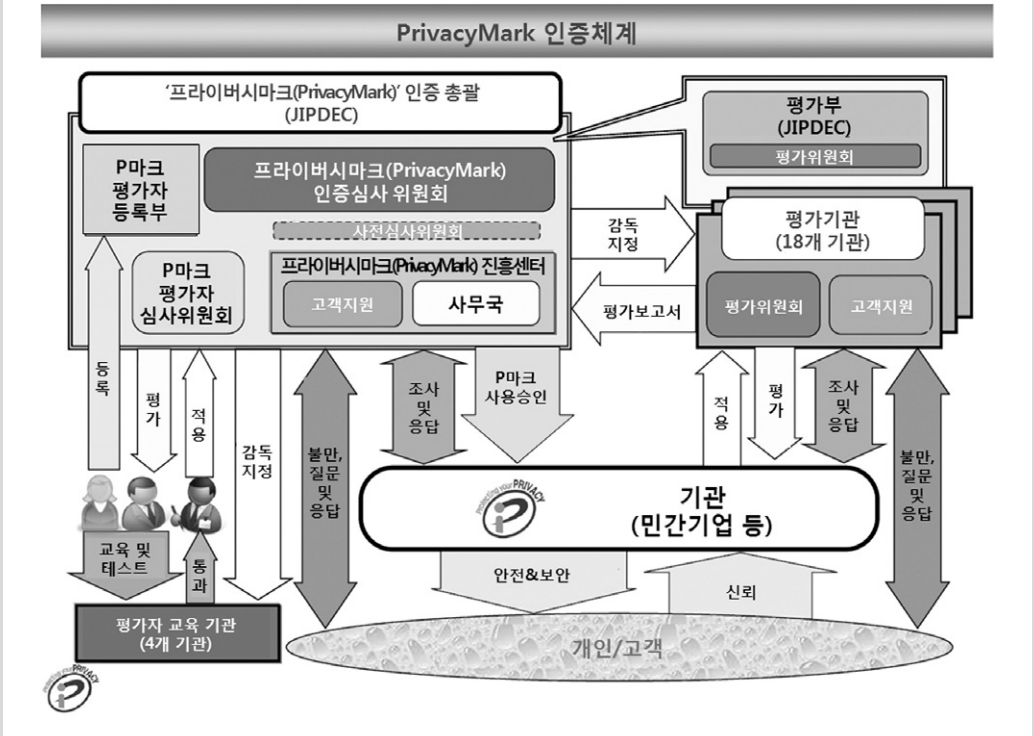
자료: 개인정보 보호 인증제 운영에 관한 규정(안전행정부 고시 제2013-45호).

시키고 소비자와 비즈니스 파트너들로부터 사회적 신뢰를 얻기 위한 목적을 지향하고 있다[22].

P마크 인증심사는 서면심사와 현장심사로 이루어지며 기준은 PDCA개념(Plan-Do-Check-Act)에 기반을 두어 서면심사에서 120개 이상의 평가항목, 현장심사에서 작업, 보안장치 각각 50개 이상 평가항목, 40개 이상 평가항목으로 구성되어 있다. P마크 인증의 유효기간은 2년으로 18개 민간사업자 단체가 심사기관으로 지정되어 인증활동을 수행하고 있으며 심사원 수도 1,200여명, 이들을 교육하기 위한 심사원 교육기관도 4개가 운영되고 있다(그림 1 참조)[23].

이러한 P마크는 농업, 임업, 어업, 광업, 건설업, 제조, 전기 · 가스 · 열공급 · 수도업, 온수 · 통신업, 도매 · 소매업 · 음식점, 금융 · 보험업, 부동산, 서비스업, 공무 등 13개 분야로 구분하여 시행되고 있으며 2013년 10월 15일현재 일

그림 1. 일본 P마크 인증체계 구성도



자료: JiPDEC(2013), The PrivacyMark System.

22) P마크제도 사이트, http://privacymark.jp/, [인용 2013.10.20].
23) JiPDEC(2013), The PrivacyMark System.

본 내 P마크를 획득한 누적 기관 수는 13개분야 13,252개, 그 중 가장 많은 분야는 서비스업으로 9,888개 기관이 획득하였고 의료기관은 47개 기관이 획득한 것으로 나타나고 있다(표 10 참조)[24]. 일본의 P마크 제도는 정부의 정책적인 인센티브 제공보다는 자율적인 문화형성 및 신뢰성 제고 효과를 꾀하고 있다.

5. 결론 및 정책과제

이상과 같이 개인정보 보호 관련하여 우리나라의 각종 인증제도와 함께 일본의 프라이버시 마크제도를 분석해본 결과, 먼저 우리나라의 인증제도는 <표 11>과 같이 미래창조과학부, 방송통신위원회, 안전행정부 등 관할부처와 이에 따른 인증기관이 나누어져 있고 PIPL제도 시행을 앞두고 있는 시점에서 이들 국내 각종 인증제도들의 평가 세부내용이 크게 다르지 않아 이를 수용하여야 하는 대상기관 입장에서는 비용적인 부담 뿐 아니라 그 실효성에 대해서도 우려를 나타내고 있다[25].

한편, 일본의 P마크제도와 비교해볼 때, 부문별 영역별로 나누어져 있지 않아 즉 영역별 특성을 반영하고 있지 않아 아직까지는 의료기관이 이러한 인증제도를 활발하게 수용하지 않고 있는 실정이다.

인증제도를 시행하는 의의는 기관차원의 필

표 10. 업종별 일본 P마크 발급현황

분류		사업자 수
계		13,252
농업		1
임업		0
어업		0
광업		0
건설업		195
제조업		1,400
전기 · 가스 · 열공급 · 수도업		16
운수 · 통신업		564
도매 · 소매업, 음식점		795
금융 · 보험업		250
부동산		143
서비스업	소계	9,888
	세탁 · 이발 · 목욕탕업	8
	주차사업	7
	기타 생활관련 서비스업	126
	여관, 기타숙소	5
	오락업	15
	자동차 정비업	5
	기계 · 가구등 수리업	34
	물품 임대업	32
	영화 · 비디오 제 작업	62
	방송업	77
	정보서비스 조사업체	5,451
	광고업	522
	전문서비스업	626
	협동조합	22
	기타사업 서비스업	2,503
	폐기물 처리업	85
	의료업	47
	보건위생	129
	사회보험, 사회복지	53
	교육	30
	학술연구기관	8
	정치 · 경제 · 문화단체	41
공무		0

자료: P마크제도 사이트 중 'P마크 부여사업자 일람', http://privacymark.jp/certification_info/list/clist.html, [인용 2013.10.20].

24) P마크제도 사이트 중 'P마크 부여사업자 일람', http://privacymark.jp/certification_info/list/clist.html, [인용 2013.10.20].
25) ZDNet Korea(2013.06.20.) http://www.zdnet.co.kr/news/news_view.asp?artice_id=20130620082009&type=det; 데이터넷(2013.10.07.), http://www.datanet.co.kr/news/articleView.html?idxno=68727.

표 11. 개인정보 보호관련 자율적, 규제적 성격의 제도현황('13.10월 현재)

구분	홈페이지 인증		정보보호 관리체계 인증	개인정보보호 관리체계 인증	
	ePRIVACY	i-Safe	ISMS	PIMS	PIPL
관련법	정보통신망법 및 개인정보 보호법		개인정보 보호법	정보통신망법	개인정보 보호법
관련고시	-		정보보호 관리체계 인증 등에 관한 고시	개인정보보호 관리체계 인증 등에 관한 고시	개인정보 보호수준 인증 등에 관한 고시
시행시기	2000년	2002년	2002년	2010년	2013년
의무사항 여부	자율	자율	의무(일정규모이상 정보통신사업자)	권고	권고
대상	기업 및 기관 홈페이지		정보통신사업자	정보통신사업자	공공 및 의료, 금융영역 민간기관
주관기관	개인정보보호협회		미래창조과학부	방송통신위원회	안전행정부
인증기관			한국인터넷진흥원	한국인터넷진흥원	한국정보화진흥원
인증항목수	86개 항목	136개 항목	104개 항목	124개	65개
유효기간	1년	1년	3년	3년	3년
유효 인증기관수	138기관	58기관	133기관	29기관	-

요한 조건들을 갖추어 가는 것도 있으나 무엇보다도 제시된 기준에 도달하기 위해 필요한 절차와 조건들을 학습하고 이행하는 과정에서 조직 구성원들의 의식과 행동양식이 개선되고, 궁극적으로는 조직의 개인정보 보호수준이 향상됨에 있다고 할 수 있다.

의료기관에서의 개인정보 보호, 개인의료정보 보호는 제고의 여지없이 중요하고도 필요한 과제이나 아직은 많은 기관들이 이러한 자율규제적인 인증제도에 선뜻 참여하지 않고 있다. 이는 다른 영역과 비교하여 인식측면에서, 환경측면에서 더 많은 준비가 필요하다고도 할 수 있을 것이다. 그러므로 이제 막 출발점을 내딛고 있는 PIPL 제도에서 의료영역이 대상 영역 중 하나로 자리잡기를 바라며 다음과 같은 준비과제를 제안하고자 한다.

첫째, 의료기관의 개인정보보호 관리현황에 대한 주기적인 실태파악이 필요하다

먼저 기관의 개인정보보호 관리체계에 있어 문제점, 취약점 등을 파악하여 개선방안을 모색하기 위해서는 의료기관 종류별 개인정보보호 관리현황 파악이 필요하다. 현재 정보화현황에 대해서는 심사평가원이 조사사업을 통해 주기적으로 실태파악을 하고 있으나 개인정보보호 관리현황에 대해서는 일부 연구에서 가능한 의료기관을 대상으로 한 조사는 수행되고 있으나 전국적 규모의 조사는 이루어지지 않고 있으며 그 참여율도 매우 낮은 편이다. 그러므로 의료영역, 의료기관의 개인정보보호 관리수준이 일정 궤도에 오르기까지 문제점을 파악하고 해결안을 모색하기 위해 정부 및 공공기관이 주도하여 주기적인 개인정보보호 관리실태 파악을 제안해본다.

둘째, 의료기관 종류별 맞춤형 필수 관리지침

개발 및 보급이 필요하다.

인증이라는 것은 정해진 기준에 적합한지 여부를 평가하는 것이라 할 수 있는바, 이는 다시 말해 정해진 기준은 하나의 지침이 될 것이다. 현재 의료기관용 개인정보보호 가이드라인이 마련되어 있기는 하나 의원, 병원, 종합병원, 요양병원 등과 같이 의료기관의 특성을 반영하지 않고 일괄 적용하고 있어 현장에서 그대로 사용하기에 아쉬운 점이 있고 또한 개인정보 보호법에 대한 모든 내용을 담고 있다보니 의료기관이 특히 취약한 영역에 있어서 보다 상세한 내용을 담지 못하고 있다. 그러므로 개인정보보호관리에 대한 실태파악현황 결과 나타난 문제점 및 취약점을 중심으로 한 특성별 관리지침마련이 필요하다. 한편, 개발된 관리지침은 대한병원협회, 대한의사협회, 중소병의원협의회, 대한병원정보협회, 시도 및 시군구 의사회, 전문과목별 의사회등 관련 협 · 단체 등을 통한 적극적인 보급활동 또한 필요할 것이다.

셋째, 의료기관별 맞춤형 컨설팅 및 교육이 필요하다.

의료기관은 직원수가 최소 2인으로 구성된 의원급에서부터 직원수가 7,000~8,000명에 이르는 상급의료기관까지 매우 다양하며 개인정보보호업무 담당자도 의원의 원장 의사선생님에서부터 종합병원의 원무과 직원, 의무기록팀 직원, 홍보과 직원, 전산팀 직원 등 까지 매우 다양한 양상을 띠고 있다. 반면 개인정보 보호업무는 제도적, 관리적, 기술적 측면을 다 포함하고 있어 기관에 따라서는 개인정보 보호업무에 대한 이해도 차이가 많이 날 수밖에 없다. 그러므로 이러한 의료기관 특성에 맞는 맞춤형 컨설팅과 아울러 인식제고, 기술이전 등을 위한 교육이 필요하다.

마지막으로 넷째, 앞에서 언급한 주기적인 현황파악, 맞춤형 관리지침 개발 및 보급, 맞춤형 컨설팅 및 교육, 그리고 의료영역에서의 개인정보보호 규제준수를 관리 · 감독할 수 있는 보건복지분야 개인정보 보호 전문기관 육성이 필요하다 하겠다. 현재 국가적 차원의 제반 개인정보 보호업무 및 활동 수행에 있어 관련 법에 근거하여 한국인터넷진흥원, 한국정보화진흥원 등이 지정되어 있다. 그러나 보건복지분야에는 이를 위한 충분한 예산 및 별도의 전문기관이 지정되어 있지 않아 많은 활동을 펼치지 못하고 있다. 그러므로 개인정보 보호 측면에서 특히 중요한 의료분야, 더 나아가 보건복지분야의 개인정보 보호 업무 및 다양한 활동을 안정적이고 지속적으로 수행하고 적극적인 홍보와 더불어 개인정보 보호 규제준수를 관리 · 감독하기 위한 보건복지분야 개인정보보호 전문기관 육성이 필요하다 하겠다.

이상과 같은 제반 선행과제 수행을 통해 의료기관의 개인정보 보호에 대한 인식제고와 더불어 개인정보 보호에 대한 기술적, 관리적 환경이 조성되어 개인정보 보호 인증제도가 활성화되고 아울러 개인정보 보호 수준이 한층 향상될 것이다. 보건복지