의료정보보호를 위한 법률과 방안

우성희

한국교통대학교

Security and Law for Medical Information

Sung-hee Woo

Korea National University of Transportation

E-mail : shwoo@ut.ac.kr

요 약

최근 IT, BT, NT 등의 융합과 정보시스템의 비약적 발전으로 정보통신 서비스가 활성화되면서 SNS, 클라우드 서비스 등 신규서비스가 증가함에 따라 개인정보의 유출위험이 증대되고 있다. 특히 IT와 의료 분야는 지속적인 경제 발전과 고령화 사회 진입으로부터 발생되는 문제를 해결하고 삶의 질 향상에 대한 요구에 따라 IT 기술을 활용한 새로운 의료기기 및 유헬스 서비스의 새로운 시장을 형성을 기대할 수 있다. 하지만 이러한 IT 기술의 도입으로 대부분의 의료 정보 시스템이 전산화 되면서 의료기관간에도 의료정보정보의 교환 및 전송이 자주 발생함에 따라 의료 정보유출 및 보안에 대한 위험성이 커지고 있다. 따라서 본 연구에서는 개인 의료정보 보호와 관련 주요 법 제도와 관리적, 기술적 보호 방법을 검토 및 분석한다.

ABSTRACT

The risk of leakage of personal information is growing with new services such as social networking and cloud services by the rapid development of information. In particular, the field of medical IT technology is required to solve problems arising from the aging society and sustainable economic development, and in accordance with the requirements to improve the quality of life, a new market for medical devices and healthcare services can be expected. However, most of the medical information system was computerized with the introduction of IT technology, and when they exchange and transfer of medical information between institutions, medical information leakage occurs and security risk is growing. In this paper we review and analyse the security of personal health information related to the major legal systems and technical and administrative protection.

키워드

의료정보보호, 의료정보 시스템, 유헬스케어, 개인정보보호

Ⅰ. 서 론

정보시스템의 발전으로 정보통신 서비스가 활성화되면서 SNS, 클라우드 서비스 등 신규서비스가 증가함에 따라 개인정보의 유출위험이 증대되고 있다. 실제로 외부 해킹에 의한 개인정보 유출도 2011년 후반에만도 C월드 3,500만명, N슨 1,320만명 등 수천만명의 개인정보 유출사고가 발생되고 있어 정보보호의 중요성이 증대되고 있다[1]. 다행히 개인정보보호법이 2012년 9월 개정 시행됨에 따라 법적 규제가 강화되고 있고 이용자 스스로 자기정보를 스스로 통제할 수 있도록 하는 사회적 분위기가 조성되고 있다. 또한 2012년 2월 주민번호 수집금지 입법이 공포되어 주민번호를 대체할 수 있는 기술적인 대체수단이 적용되고 있고 수집된 개인정보도 개인정보 유효기간제를 적용하여 불필요한 개인정보 보관을 최소화하기 위해 일정기간 미 이용자의 개인정보를 파기토록 하는 등 필요한 조치를 법제화 하고 있다. 개인정보 이용내역에 관련하여서도 주기적으로 이용내역을 정보주체에게 통지하여 개인정보의 침해사고 발생 시에도 2차 피해 확산을 방지하도록 하고 있다.

특히 IT와 의료 분야는 지속적인 경제 발전과

고령화 사회 진입으로부터 발생되는 문제를 해결하고 삶의 질 향상에 대한 요구에 따라 IT 기술을 활용한 새로운 의료기기 및 유헬스 서비스의 새로운 시장을 형성을 기대할 수 있다. 하지만 이러한 IT 기술의 도입으로 대부분의 의료 정보 시스템이 전산화 되면서 의료기관간에도 의료정보 정보의 교환 및 전송이 자주 발생함에 따라 의료정보유출 및 보안에 대한 위험성이 커지고 있다.

본 연구에서는 개인 의료정보 보호와 관련 주요 법 제도와 관리적, 기술적 보호 방법을 검토 및 분석한다.

II. 의료법 적용법령 및 주요 조치사항

행정안전부와 보건복지부 의료기관이 환자의 정보를 안전하게 보호·관리하기 위한 기준과 원칙을 담은『의료기관 개인정보보호 가이드라인』이 발간하고 진료정보의 수집·관리·제공·폐기 등 개인정보보호 업무 단계별 처리요령, CCTV 설치·운영 방법 등을 의료기관의 특성에 맞추어 설명하고 있다. 가이드라인 주요 내용으로서 개인정보 보호 원칙 및 처리 기준 소개하고 표1~ 표3과 같은 개인정보 처리단계별 조치요령 및 관련 사례 등 소개하고 있다. 또한 필수 서식 및 개인 정보 보호법, 의료법 등 관련 법령을 소개하고 있다. 여기에서 진료정보란 진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보 즉 진료기록부, 수술기록부, 조산기록부, 간호기록부, 환자명부 등을 의미한다.

표 1. 의료법 적용법령 및 주요 조치사항(1)

구분	진료정보	일반 개인정보
개념	•진료를 목적으로 수집하여 처리하는 개인정보가 포함된 정보 – 진료기록부, 수술기록부, 조산기록부, 간호기록부, 환자명부 등	•홈페이지 회원정보, 홍보를 위한 연락처 등 일반 개인정보
일반 원칙	•의료법에 규정이 있는 경우 의료법을 우선 적용 – 규정이 없는 경우 개인정보보호법 적용	•개인정보보호법을 적용
수집·이용	•의료법 제22조(시행규칙 제14조) – 동의 없이 수집 가능 – 진료목적으로만 사용 가능	•개인정보보호법 제15조 – 동의를 받아 수집

표 2. 의료법 적용법령 및 주요 조치사항(2)

구분	진료정보	일반 개인정보
관리	•개인정보보호법 – 제26조:문서로 위탁하여야 하며 위탁사실을 공개하여야 함 – 제29조:안전한 관리를 위해 접근통제, 암호화, 접속기록보관, 물리적 보호조치 등 안전성 확보조치를 하여야 함 – 제30조 : 개인정보처리방침을 수립하여 공개하여야 함 – 제31조 : 개인정보보호책임자를 지정하여야 함	
제공·열람	•의료법 제21조 – 의료법에서 지정하는 경우*외에는 제공이나 열람할 수 없음 * 가족·대리인 요청, 특별규정(열거주의)	•개인정보보호법 제18조 – 개인정보보호법에서 지정하는 경우*외에는 제공할 수 없음 * 다른 법률 근거 시 제공 가능
정정·삭제 등 요구사항 처리	• 의료법 제22조 – 법에따라 수집하는 정보이므로 정정·삭제 할수 없음	•개인정보보호법 제35조, 제36조 – 법에서 정한 사유 외에는 정보주체의 열람·정정·삭제 등 요구에 응하여야 함

표 3. 의료법 적용법령 및 주요 조치사항(3)

구분	진료정보	일반 개인정보
보관 및 파기	• 의료법 시행규칙 제15조 – 법에서 정한 최소 보유기간 이상 보관하여야 하며 진료목적상 필요시 연장보관 가능	• 개인정보보호법 제21조 – 보유목적이 달성되면 즉시 파기
이관	• 의료법 제40조 – 폐업이나 휴업시 관할 보건소장에게 진료기록 이관 – 보건소장의 허가를 받은 경우 의료기관 개설자가 계속 보관 가능 ※ 허가사항 변경시는 의료기관이 유지되는 것으로 봄	• 개인정보보호법 제27조 – 의료기관 변경시 정보주체에게 이관사실을 알려야 함
유출, 침해 대응	• 개인정보보호법 제34조, – 정보주체에게 유출사실을 알리고 1만건 이상일 경우 행정안전부 또는 전문기관(KISA, NIA)에 신고 • 개인정보보호법 제62조, – 정보주체가 침해신고센터에 침해사실을 신고한 경우 조사에 협조	
영상정보처리기기 운영	• 개인정보보호법 제25조 – 대기실 등 공개된 장소에 CCTV 설치시 반드시 안내판을 설치 • 개인정보보호법 제15조 – 진료실, 수술실 등 비공개 장소에 CCTV를 운영하려면 정보주체의 동의를 받아야 함	

III. 생명주기에 따른 의료정보 보호법

개인 의료정보의 누출에 따른 피해를 최소화하기 위해서는 의료기관의 특성을 고려한 효율적인 개인정보 생명 주기(수집. 이용, 제공, 위착, 영업양도, 양수,관리 파기, 이용자 관리)에 따른

관리적, 기술적인 처리가 필요하다. 우선 작년 2012년에 개정된 의료법[3]과 정보통신망법과 비교하면 다음 표 4과 표5와 같다.

표 4. 의료정보 생명주기에 따른 정보보호법(1)

생명주기		의료법	정보통신망법
수집	정보수집	진료목적으로 동의없이 수집 가능(진료기록부등)	이용자 동의
	초소한의 정보수집		규정
	민감정보수집	진료목적으로 동의없이 수집 가능(진료기록부등)	별도 동의 획득
	주민등록번호수집		주민등록번호 사용, 이용 금지
	아동의 정보수집		법정대리인의 동의
이용			이용자 동의 없는 목적외 이용금지
위탁	제공	국민건강보험 등 동의 없이 제공가능	이용자 동의
	일반위탁		수탁자,위탁업무 등 위탁사실 공개
	홍보,판매등의 위탁		이용자대상 위탁사실 동의(서비스 이용 계약 외 위탁)
	수탁자 감독		안전성 조치 등 문서화

특이사항으로 개인 정보 수집시 또한 주민번호의 수집 및 이용을 금지하고 있다. 예외적으로 본인 확인기관으로 지정되거나 법령에서 허용하거나 방통위 고시가 되었을 경우는 예외적으로 허용한다. 주민 번호의 대체 수단으로 아이핀이나 휴대폰, 공인인증서등을 권장하고 있다. 따라서 주민번호 사용제한을 위해 많은 준비 절차가 필요하다. 개인정보제공 단계에서는 개인 정보를 개인 정보 취급자 외에 제 3자에게 제공하거나 위탁시 제 3자의 이익이나 사업목적 달성을 위해 제 3자에게 개인 정보를 제공하는 경우나 수탁자에게 개인 정보를 제공하는 경우 제 3자에게 고지할 의무와 이용자에 대한 동의 의무, 위탁 사실 고지 및 동의 획득이 있어야 한다. 단 법령 근거 있는 개인 정보 제 3자 제공은 동의 절차가 불필요하다. 또한 동의 없이 제공이 가능한 경우는 환자의 배우자, 직계 존비속, 배우자의 직계존속, 대리인이 환자본인의 동의서 및 증명서등을 첨부하여 요청하는 경우이며 환자가 사망 또는 의식이 없는 등 동의를 받을 수 없을 경우나 건강 보험 요양급여비용 청구를 위해 건강 보험 심평원에 주민 번호 등 개인정보가 포함된 요양급여 비용 명세서를 제출하는 등의 예외적인 사항이 있다.

영업의 양수, 양도에 있어서도 이전 사실을 홈페이지에 게시나 전자우편으로 전송하여 고지를 해야 한다.

표 5. 의료정보 생명주기에 따른 정보보호법(2)

생명주기	의료법	정보통신망법
영업 양도, 양수		이용자 고지
관리	전자의무 기록 관리, 보존에 필요한 장비 규정	기술적, 관리적 보호조치(외부 인터넷망과 망분리)
		개인정보관리 책임자 지정
		개인정보 취급 방침 공개
		개인정보취급자 연2회교육(고시)
파기		보유기간 경과 및 목적 달성 시 파기
	진료기록 보존 기간 규정 (진료기록부 10년, 환자명부 5년 등)	개인정보 유효기간 제도
이용자 권리	환자 동의 및 관계 증명서 첨부시 진료기록 열람, 제공	열람,정정,동의 철회 권리 보장
		개인정보 이용내역 통지
		개인정보 누출 등 통지, 신고

Ⅳ. 의료정보의 보호 조치

개인정보 관리를 위해서는 관리 책임자를 지정하고 개인 정보보호 및 이용자 고충을 처리하도록 하며 종업원이 5명 이내일 경우 사업주가 겸임가능하며 개인 정보 방침에 쉽게 확인 가능하도록 책임자를 공개한다. 담당자는 개인정보 분실 및 도난, 누출 등 사실이 있다면 바로 이용자에게 통지 및 방통위에 신고해야 한다. 내부 관리 계획에 포함되어야 할 사항은 개인 정보 관리 책임자의 자격 요건 및 지정이 포함되어있어야 하며 개인 정보 관리 책임자와 개인 정보 취급자의 역할 및 책임, 개인 정보 내부관리계획의 수립 및 승인, 개인정보의 기술적, 관리적 보호 조치 이행 여부의 내부점검, 그 밖의 개인 정보 보호를 위해 필요한 사항, 개인정보보호 교육계획 수립 및 년 2회 이상의 교육실시, 보호 조치 이행을 위한 세부적인 추진방안 등이 포함되어야 한다.

개인 정보의 기술적 관리 조치로는 접근권한을 제한하며 개인정보취급자 변경 시 권한을 말소 변경, 그 기록을 최소 5년간 보호 하도록 하며 안전한 인증방식을 도입하고 인증서를 이동식 저장매체에 보관하는 것이 안전하다. 아이디와 비밀번호를 이용하는 인증과 다른 특성을 갖는 인증 수단 활용이 가능한데 그 예로서 보안토큰, 휴대폰 인증, 일회용 비밀번호, 바이오 정보등이 있다.

접근 통제와 침해사고 방지를 위한 시스템으로 방화벽이나 침입탐지 시스템, 공개용 소프트웨어 알약 등이 있다. 접근 통제를 위한 또 다른 방법

은 개인 정보처리 시스템과 외부 인터넷망을 분리하는 것이다. 물리적 망 뿐 만 아니라 논리적 망 분리도 하여 일정 수준의 보안성을 갖는다.

V. 결 론

IT와 의료 분야는 지속적인 경제 발전과 고령화 사회 진입으로부터 발생되는 문제를 해결하고 삶의 질 향상에 대한 요구에 따라 융합기술의 새로운 형태로 즉, 유헬스 서비스의 새로운 시장을 형성을 기대할 수 있고 의료 정보 시스템이 전산화 되면서 의료기관간에도 의료정보정보의 교환 및 전송이 자주 발생함에 따라 의료 정보유출 및 보안에 대한 위험성이 커지고 있다.

따라서 연구에서는 개인 의료정보 보호와 관련 주요 법 제도와 의료정보의 생명주기에 따른 관리적, 기술적 보호 방법을 검토 및 분석한다

참고문헌

[1] “SNS 서비스 확산에 따른 프라이버시 침해대응방안”, 임문영, 2011 개인정보 관리책임자 및 취급자 워크숍

[2] 한국정보보호진흥원[06-05]

[3] 의료기관 개인 정보보호 가이드라인, 2012.9