情報保護學會論文誌
第 20卷 第 6號, 2010. 12

개인건강정보의 2차이용 보호에 관한 국내외 법안 연구*

박 한 나,[1†] 정 부 금,[1‡] 이 동 훈,[2‡] 정 교 일[1‡]
[1]한국전자통신연구원, [2]고려대학교 정보경영공학전문대학원

Research on the Domestic and Foreign Legislation about Secondary Use Protection for Personal Health Information*

Han-na Park,[1†] Boo-Geum Jung,[1‡] Dong-Hoon Lee,[2‡] Kyo-il Chung[1‡]
[1]Electronics and Telecommunications Research Institute, [2]Graduate School of Information Management and Security

요 약

의료서비스와 IT 기술간의 융합으로 환자 개인의 건강정보가 전자의무기록(EHR)의 보급과 함께 빠르게 전자화되고 있다. 이와 함께 유헬스사회에 접어들면서 전자화 된 환자의 건강기록들을 진료 이외의 공중보건 및 의학 분야의 연구, 의료서비스 향상을 위해 사용하고자 하는 2차이용의 요구가 증가하고 있다. 개인건강정보의 2차이용으로 의학 분야의 발전은 매우 유익한 일이지만 부주의하게 개인의 건강정보를 이용하는 경우 환자 개인의 프라이버시 손상이 발생, 더불어 2차이용을 통한 연구나 서비스 발전에도 제한이 발생할 수 있다. 하지만 아직 개인건강정보를 이용한 2차적 이용에 대해 체계적인 연구나 논의가 없는 것이 현실이다. 따라서 본 논문에서는 개인건강정보의 2차이용과 관련하여 국내외의 법안들을 살펴보고 이를 비교 분석하여 앞으로 개인의 프라이버시를 존중하고 더불어 의료분야 서비스의 발전을 도모할 수 있는 방향을 제시하고자 한다.

ABSTRACT

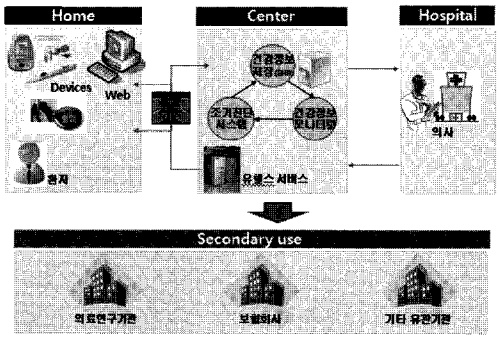
Through the convergence of medical services and the IT technique, the patient's personal health information computerization has been rapidly spread with propagation of electronic medical record(EHR). In addition, by entering u-health, the demand of the secondary use for public health, medical research, and medical service using electronic patient health care records are increasing. The personal health information secondary uses for the development of academic medical area and service, are very good thing. But, carelessly to use personal health information, the patient privacy would be damaged. However, there are not yet systematic studies about secondary use of personal health information. Therefore, in this paper, we analyze the difference of the internal and external bill for personal medical data secondary use and propose the direction of the medical service development and preservation of the individual's privacy.

Keywords: Privacy, Personal Medical data, Secondary Use, U-Health, Security

I. 서 론

최근 정보통신 기술의 발전과 의료서비스의 융합으로 의료 정보화가 가속화되고 의료기관 내에서 개인건강정보가 점차적으로 전자화되어 관리, 운영되고 있다[1]. 이와 함께 인구 고령화 추세와 건강에 대한 관심이 높아지면서 보다 편리하고 언제 어디서나 접근 가능한 의료서비스에 대한 요구가 증가하였고, 이는 유

접수일(2010년 9월 25일), 수정일(2010년 11월 9일)
게재확정일(2010년 12월 13일)
* 본 연구는 지식경제부의 지원을 받는 정보통신표준기술력 향상사업의 연구결과로 수행되었음
† 주저자, hnpark@etri.re.kr
‡ 교신저자, bgjung@etri.re.kr, donghlee@korea.ac.kr, kyoil@etri.re.kr



〔그림 1〕. 유헬스기반의 개인건강정보의 2차이용

비쿼터스 컴퓨팅과 의료 서비스가 결합한 유헬스 서비스로 나타났다. 유헬스 서비스는 언제 어디서나 환자에게 부착된 센서나 의료 기기를 통해 환자의 건강정보를 측정, 전달하여 이를 바탕으로 원격에서 의료 서비스를 제공할 수 있게 해주는 서비스를 말한다[2]. 개인건강정보의 전자화와 유헬스 서비스의 도입은 개인건강정보가 네트워크를 통해 전송되고 서버에 저장, 공유되면서 이제 직접적인 의료 서비스를 넘어 질병 예방이나, 연구 등 공중보건 및 의학 분야의 연구, 의료서비스의 질 향상과 마케팅 등 개인건강정보를 2차적으로 이용하고자 하는 요구로 나타나고 있다[그림 1].

개인건강정보는 개인신상정보나 민감한 병력정보 등 프라이버시를 침해할 수 있는 정보들이 포함되어 있는 개인정보로, 과거 의무기록의 전자화 도입 시 의료데이터의 공유 및 활용상에서 발생하는 프라이버시 문제에 대해서는 전에 논의된 적이 있었다. 하지만 개인건강정보의 2차적인 이용에 대해서는 연구가 미흡한 실정이다. 1차적인 의료기관이 아니라 제2의, 제3의 기관으로 개인의 의료정보가 전달되고 사용되어지는 것은 또 다른 접근이 필요하다. 개인건강정보의 2차이용으로 의학 분야나 서비스의 발전은 매우 유익한 일이지만 부주의하게 개인의 건강정보를 이용하는 경우 개인의 프라이버시가 손상될 수 있어 부정적인 인식이 확산될 수 있고, 결과적으로 2차적 이용을 통한 연구나 발전이 제대로 이뤄지지 않을 수 있다. 따라서 개인건강정보의 2차이용을 활성화하면서 동시에 환자 개인의 프라이버시를 보호할 수 있어야 한다.

따라서 본 논문에서는 개인건강정보의 2차이용과 관련하여 국내외의 법안들을 살펴보고 이를 비교 분석하여 앞으로 개인의 프라이버시를 존중하고 더불어 의료서비스의 발전을 도모할 수 있는 방안을 제시하고자 한다.

본 논문은 다음과 같이 구성되었다. 2장에서는 개인건강정보의 2차이용의 정의와 사용목적에 대해 알아보고, 3장에서는 국외 개인건강정보의 2차이용에 관한 법률, 4장에서는 국내 개인건강정보의 2차이용에 관한 법률에 대해 언급하고, 5장에서는 언급한 국내외 2차이용 관련 법률들을 비교 및 검토 후 6장에서 결론을 맺는다.

II. 개인건강정보의 2차이용

2.1 개인건강정보의 2차이용 정의

개인의 건강정보는 의사가 환자와 대면하여 직접적인 진료나 처방 등의 행위와 관련하여 생성되고 이를 위해 사용되는 것이 1차적인 개인건강정보의 이용이라 할 수 있다. 이와 달리 개인건강정보의 2차이용은 의료정보의 분석 및 연구, 공중보건, 지불, 인증, 마케팅, 기타 상업 활동 등 진료와는 별도로 개인의 건강정보를 이용하는 것을 말한다[3] 개인건강정보를 2차적으로 사용하는 기관은 의료기관을 비롯하여 의료분야연구기관, 제약회사, 보험회사, 지불결재 회사 등 다양한 관련기관이 존재하며, 이처럼 2차이용의 범위가 넓음을 알 수 있다.

2.2 개인건강정보의 2차이용 목적 분류

개인건강정보를 2차적으로 이용하는 용도는 그 목적에 따라 크게 세 가지로 나누어 볼 수 있다([표1]참조). 먼저 건강문제의 경향을 파악하거나 인구생체계측, 희귀병의 등록 및 연구 등 공중보건의 발전과 의

〔표 1〕 개인정보의 2차이용 목적

구 분	사 용 목 적
공중보건 및 연구목적	- 공공보건 보호 및 강화 - 건강관련연구개발 - 희귀질병 및 불치병 연구 - 의료 용어생성 및 유지
환자 개인 진료향상 목적	- 환자진료의 질 관리 - 환자안전향상 연구 - 개인건강관리 - 건강관리제공자를 위한 의사결정 지원개발 및 적용서비스 개발
기 타	- 보안 및 기밀성 알고리즘 개발 - 재정상태 분석 및 관리 - 위반 및 부적절한 감시활동 - 시장조사 및 마케팅

료기술의 연구를 위해 사용하는 경우이다. 둘째로는 환자 개인관리의 질적 향상을 위해 개인에게 맞춤 서비스를 제공하기 위한 용도이다. 마지막으로 보험회사나 의료기관 등에서 의료마케팅이나 서비스의 안전성 분석, 재정상태 분석 및 관리 등을 위한 기타용도가 있다.

2.3 개인건강정보의 2차이용 시 요구사항

개인건강정보는 개인의 일반적인 인적사항을 포함하여 성적인 질병 등 민감한 병력사항 등을 포함하고 있어서 단순히 개인정보보호의 측면과 다른 접근이 필요하다. 또한 의료 서비스를 비롯하여 의료분야의 연구를 위해서 의사, 환자 뿐 아니라 연구소, 행정기관 및 정부기관들 다양한 기관들이 개인건강정보를 공유한다는 점도 고려해야 할 요소이다. 따라서 개인건강정보는 건강정보의 특성과 1차적 혹은 2차적 이용 등 그 용도에 따라서 다른 접근이 필요할 것이다. 최근 송유진 외는 크게 개인건강정보의 데이터 측면에서의 보호와 환자개인의 프라이버시 보호를 위한 측면으로 나누어 의료데이터 공유 및 활용 서비스를 위한 보안/프라이버시 요구사항을 제안하였다[4]. 데이터의 측면에서 데이터의 기밀성, 무결성, 가용성을 보장해야 하며, 프라이버시 측면에서 익명성, 비연결성, 식별 불가능성, 세밀한 접근 제어 등을 갖출 것을 [표 2]과 같이 요구하였다.

이와 더불어 2차적 이용에 참여하는 객체들의 역할 및 책임과 관련하여 개인건강정보 주체, 2차적 사용자, 정부 등 중앙관리기관 으로 나누어 보안요구사항을 제시하고자 한다.

2.3.1 개인건강정보 주체

개인건강정보는 환자와 의사가 직접적으로 대면하여 진료 및 검사 등 의료행위를 통해 생성된다. 환자 개인마다 주민번호와 같은 개인 식별을 통해 정보가 관리되며, 그 내용이 환자마다 개별적으로 기록됨으로 개인건강정보의 주체를 환자 본인이라고 볼 수 있으며 다음과 같은 권리를 반드시 보장해야 한다.

- 본인의 개인건강정보에 대해 열람이 가능해야 한다.
- 본인의 개인건강정보에 대해 공유, 활용 등에 있어 정보의 제어 및 의사를 표현할 수 있어야 한다.
- 개인건강정보의 기밀성 및 무결성을 보장받아야 한다.

2.3.2 개인건강정보의 2차 사용자

의료분야의 연구나 의료 서비스 발전을 위해 개인의 건강정보를 사용하는 2차적 사용자의 경우 그 목적과 이유에 따라 다를 수 있겠지만 최소한 다음과 같은 의무 사항을 지켜야 한다.

- 개인건강정보의 열람 시 정보주체에게 통지 및 동의를 구해야 한다.
- 전달받은 개인건강정보에 대해 안전하게 관리, 보존해야 한다.
- 개인건강정보를 통해 직, 간접적으로 알게 된 사실에 대해 비밀을 유지해야 한다.
- 해당 목적에 맞는 범위 내에서 개인건강정보를 얻어야 하며 프라이버시침해가 최소가 되도록 해야 한다.

[표 2] 의료데이터 공유 및 활용서비스를 위한 보안/프라이버시 요구사항[4]

	기본방향	기본 요구사항
데이터보안	-기밀성 보장 -무결성 보장 -가용성 보장	의료 데이터는 안전하게 저장되어야 함
		외부 공격자의 침입을 통한 데이터가 불법으로 유출되어서는 안 됨
		내부자에 의한 데이터 유출이나 실수에 의해 데이터가 유출되지 않도록 해야 함
프라이버시 보호	-익명성 보장 -연결 불가능성 보장 -식별 불가능성 보장 -세밀한 접근 제어	의료 데이터는 익명으로 저장될 필요가 있음
		의료 데이터에 대한 접근제어 기능이 보장되어야 함
권한 관리 보호		의료 데이터에 대한 접근 시 세밀한 접근제어 기능이 제공될 필요가 있음
		의료 데이터는 안전하게 공유되어야 함
		의료 데이터 소유자의 소유권 등 지적재산권 보호가 필요함

2.3.3 개인건강정보의 중앙관리 기관

환자가 믿고 신뢰할 수 있으며, 2차적으로 이용하는 사용자가 적절한 개인건강정보를 사용할 수 있도록 감독 및 관리의 기능을 담당하고 있는 중앙관리 기관의 경우 다음의 사항이 요구된다.

- 개인건강정보를 2차적으로 이용하고자 하는 경우 승인 및 인증절차를 거치도록 해야 한다.
- 개인건강정보의 효과적인 보호를 위해 개인 식별 정보의 민감도를 세부적으로 정의해야 한다.
- 개인건강정보의 안전한 2차이용을 위해 최소한의 프라이버시침해가 일어나도록 법적으로 보호해야 한다.

III. 국외 개인건강정보의 2차이용 관련 법률

3.1 미 국

미국의 경우, 개인건강정보보호와 관련하여 기본 바탕으로 의료관련 전자정보교환과 건강정보의 보호(Privacy), 보안(Security)에 관한 법률인 HIPPA (Health Insurance Portability and Accountability Act of 1996)를 가지고 있다[5]. 이후 미국연방정부 산하의 보건후생성의 개인적으로 식별 가능한 건강정보의 비밀보호를 위한 표준이 사생활보호법(Privacy Rule)으로 변경, 표준에서 법률로 발전하였으며, 미국 전역에서 적용되는 최소한의 법률로 쓰이고 있다[2]. 또한 보건후생성 내에 인권국을 통해 사생활보호법을 반드시 준수하도록 집행하고 감독하고 있다[3].

특히 미국에서는 공공 보건 연구와 테러리즘 대비, 질병발생 감시 등과 관련하여 개인건강정보의 2차이용이 증가하고 있다. 2차이용은 그 목적이 다양하여 어떠한 법률을 적용해야 하는지는 상황에 따라 다를 수 있지만 기본적으로 피험자 보호 법률과 사생활보호법을 반드시 준수해야 한다. 사전의 개인건강정보의 소유주에게 이용과 공개에 대한 동의를 구하는 것을 기본으로 특히 연구, 공공의료 혹은 의료서비스의 운영과 관련된 목적을 위해서는 HIPPA가 지정한 개인식별정보(이름, 주소, 사회보장번호 등)가 제거되거나 삭제된 데이터를 제한적으로 사용하도록 명시하고 있다[4]. 또한 제한된 데이터를 이용할 수 있는 기관에 대해 사용목적 공개와 허용된 데이터의 기밀성, 정보의 남용 혹은 부적절한 공개 방지를 위한 적절한 조치를 취할 것에 대한 동의를 받도록 요구하고 있다. 이와 더불어 개인건강정보를 통해 개별적으로 얻는 이득이 제한되도록 정보의 접근, 검색, 접근권한 설정을 정하는 과정을 복잡하고 어렵게 하여 개인 식별 가능한 의료정보에 대한 접근을 제공하지 못하도록 하고 있다.

특히, 개인건강정보의 2차이용의 효율성을 지원하기 위해 개인건강정보를 통한 연구나 활용에 있어 준수해야 할 지침을 제시하고 있다[6].[표3]

이 외의 연방정보나 주에서 개인건강정보를 보호하기 위해 모델이 되는 법의 형태로 제시한 Model State Public Health Privacy Act와 각 관련기관에서 자신들의 실정에 맞는 매뉴얼로 작성한 NCHS (National Center for Health Statistics) Staff Manual on Confidentiality가 있다.

[표 3] 미국 PHDSC의 개인건강정보의 2차이용 지침

- 누가 건강정보를 공개하는가?
  - ① 공중보건당국
  - ② Healthcare Provider
  - ③ Health Plan
- 어떤 건강정보가 공개되는가?
  - ① 개인적으로 식별가능한 건강정보
  - ② 건강정보(정신건강, 약물중독, AIDS 등)
  - ③ 공공보건정보(통계, 전염병, 질병 등록 등)
  - ④ 기타
- 건강정보의 공개 목적은 무엇인가?
  - ① 치료, 진료비지불, 건강관리 운영
  - ② 개인적인 치료를 위한 통지 목적
  - ③ 법에서 요구하는 경우
  - ④ 건강 및 안전에 대한 위협에 대한 예방
  - ⑤ 연구
  - ⑥ 마케팅, 기금 모음, 비즈니스 등
- 어떤 요구사항 및 조건을 지켜야 하는가?
  - ① 연방정부의 소환장
  - ② 환자 동의/인증이 있는/없는 기회 또는 대상
  - ③ 최소한의 필수적 요구사항의 적용 가능성
  - ④ 공개 요구사항의 설명의 적용 가능성
  - ⑤ 특별한 주 법률 고려사항

2) 45 CFR Part160 and Part164, Subparts A and E

3) USA. Department of Health & Human Service. Protecting Personal health information in Research: understanding the HIPPA Privacy Rule. NIH Publication number 03-5388.

4) 최소필요기준의 내역은 42 CFR Section 164.514(d)에 언급하고 있다.

3.1.1 미국의 AMIA

미국의 경우 개인건강정보의 2차이용과 관련하여 AMIA(American Medical Informatics Association)을 구성하여 2차이용의 범위를 지불(Payment), 환자안전 및 질, 해석(Analysis/ quality, patient safety measurement), 공급자 인증 및 인가(Provider certification/ Accreditation), 마케팅 및 상업적사용(Marketing, other Business or Commercial Use), 연구(Research), 공중보건(Public Health) 등 6가지로 분류하여 관리하도록 하고 있다.[5] 특히 HIPPA의 사생활 보호법(Privacy Rule)에 근거하여 각 분류에 대해 다시 또 세부 사항으로 구체적으로 제시하고 있으며, 의료정보가 각 목적을 위해 사용될 경우 개인건강정보에 대한 사용뿐 아니라 공개에 대해 최소한으로 할 것을 명시하고 있다.[6] 그 중 공중보건의 경우 공중보건활동을 위한 공중보건기관이 사용하는 경우, FDA나 FDA의 관할권을 가진 개인의 경우, 아동학대나 인권유린과 관련한 보고서 작성을 위한 경우 전염병확산과 관련된 위험을 알리기 위한 경우, 직장환경의 개선을 위해 사용되는 경우로 분류하여 최소한의 정보가 노출되도록 보장하고 있다. 하지만 각 분야의 적절한 활용을 위해 별도의 조항을 가지고 있으며, 다음의 경우에 한하여 환자의 동의 없이 개인건강정보를 사용할 수 있도록 하고 있다.

- 법에 의해 요구되는 경우(§164.512(a))
- 남용 및 학대 피해자와 가정폭력 및 방치를 알려야 하는 경우(§164.512(c))
- 감사 및 감독 활동의 경우(§164.512(d))
- 상속 및 유산과 관련하여 사용되는 경우(§164.512(g))
- 시체기증과 안구, 근육 등 장기기증과 관련하여 사용되는 경우(§164.512(h))

3.2 영 국

영국은 개인건강정보보호와 관련하여 정보보호법(Data Protection Act)을 제정하여 공공과 민간의 구분 없이 영국 내에서 이루어지는 모든 개인정보 처리에 적용되는 통합법의 형식으로 운영되고 있다. 특히 개인건강정보와 관련하여 정보보호법 2조에서 민감한 정보로 분류하여 정보 소유주의 동의 없는 수집을 원칙적으로 금지하고 있다[7]. 영국은 이 법을 근간으로 개인의 건강기록, 의료 정보 등에 관한 규율조항을 별도로 가지고 있다.

개인건강정보의 2차이용과 관련하여 의료연구를 위해 정보의 보관 및 재사용할 수 있는 특수한 자유가 필요함을 인정하고 광범위한 피해나 걱정을 야기하지 않는 범위내의 연구에 대해 특수한 예외조항을 가지고 있다[8]. 무엇보다 영국의 경우 의무기록 사용에 관한 사전 공지를 제공하는 조치를 강조하여 모든 환자들이 그들의 기록이 어떻게 사용되는지를 인식할 수 있도록 하고 있다. 또한 이름 및 개인정보가 공개되기 전에 환자의 명시적 동의를 구해야 한다.[9] 특히 영국의 경우, 환자의 개인건강정보의 대해 비밀유지에 관한 관습법과 공정함의 일반적인 개념을 따르도록 하고 있다. 이와 관련하여 영국 의학연구위원회는 윤리문제에 대한 지침을 제공하는 의학연구 윤리시리즈를 발표하고 연구목적으로 개인의료정보를 사용하고자 하는 경우 상세한 연구계획서를 제출하여 승인받도록 하고 있다[6].

3.3 일 본

일본은 개인정보보호 관련 5개 법률과 공공과 민간 부분을 포괄하는 개인정보의 보호에 관한 법률을 가지고 있다[10]. 특히 공공기관의 경우 행정기관이 보유하는 개인정보의 보호와 독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률을 가지고 있다. 개인정보를 이용하는 경우 그 목적과 범위를 명확히 하고 다른 목적으로 이용하고자 하는 경우 새롭게 동의를 얻어야 함을 명시하고 있다. 또한 개인정보가 제 3자에게 제공되는 경우 사전에 동의를 구해야 하지만 타인의 생

5) Payment §164.506, Analysis/Quality /Patient Safety Measurement §164.501 (¶1), Provider Certification/Accreditation §164.501 (¶2), Marketing purposes §164.508(a)(3), Research §164.508, §164.512(i)(1)(ii)-(iii), 164.514(a)-(c), 164.514(e) 등 각 분야를 다루고 있다.

6) HIPPA Privacy Rule. §164.506

7) 환자는 자신의 개인정보가 어떻게 사용되는지, 의료서비스에 대한 전반적인 관심사항들을 제시 및 논의할 수 있도록 정보를 제공받아야 하며, 2001 MRC 웹사이트에서 이에 해당하는 정보를 얻을 수 있다.

8) 정보보호법(Data Protection Act), 1998 제33조 예외사항

9) Peter Carey, Blackstone's Guide to data Protection Act 1998, Blackstone Press, Ltd, 1998

10) 한국법제연구원, 개인정보보호법제에 관한 입법평가, 2008

〔표 4〕 국내외 개인건강정보의 2차이용 관련 법안 비교

요구사항	세부사항	미국	영국	일본	한국
개인건강정보주체	2차이용 관련 환자의 동의 유무	O	O	O	O
2차 사용자	2차이용 관련 사용목적의 사전 공지 및 공개 유무	O	O	O	X
	2차이용 시 정보의 접근권한 설정	O	O	X	X
	2차이용 시 기밀성 보장	O	O	O	O
	2차이용 시 무결성 보장	O	X	X	O
중앙관리기관	2차이용 관련 개인건강정보보호법안 유무	O	X	X	X
	2차이용 감독기관 및 승인/인증기관 존재 유무	O	O	O	O
	2차이용 관련 민감한 개인 식별 정보의 세부 정의	O	O	X	X

명, 신체 또는 재산의 보호를 위해 필요한 경우 본인의 동의 없이도 제공할 수 있으나 적절히 운용할 것을 요구 하고 있다. 특히나 민감한 정보에 관련하여 따로 개인정보를 구별하지 않고 모든 정보에 대해 개인의 인격존중을 위해 신중히 취급하며, 최소한도로 접근할 것을 규정하고 있다[11].

특히 일본 국민보험조합의 개인정보 취급 가이드라인에 따라 개인건강정보의 2차이용에 관련하여 이용목적을 사전에 통지하고 공표하도록 하고 있으며, 일본 연구윤리지침에 따라 그 이용목적을 가능한 특정짓도록 하고 있다[12]. 또한 과거 병력에 대해서는 꼭 필요한 범위에 대해 환자 본인으로부터 취득할 것을 권하고 있다. 이와 함께 개인건강정보의 기밀성과 무결성을 보장하기위해 인적, 조직적, 물리적, 기술적 안전관리 조치를 요구, 해당조치를 준수하도록 감독하도록 하고 있다[13].

IV. 국내 개인건강정보의 2차이용 관련 법률

개인건강정보와 관련하여 포괄적인 개념인 개인정보보호 관련 법률과 건강정보를 취급할 때 고려되는 건강정보보호 관련 법률, 의료연구와 관련한 법률 로 나누어 언급하고자 한다.

4.1 개인정보보호를 위한 법률

우리나라의 경우 지난 1994년 공공기관의 개인정보보호에 관한 법률이 제정되어 정보의 처리 또는 송, 수신 기능을 가진 장치에 의해 처리되는 개인정보를 보호하도록 하고 있다. 정보의 수집, 이용, 제공, 파기와 전반적인 보호를 위해 정보 활용의 준수원칙을 제시하고 있다.[7,8] 기본적으로 개인의 인권을 침해할 개인정보를 수집하지 못하도록 하고 있으며, 기밀성 및 무결성을 갖도록 하여 개인정보의 남용과 프라이버시 침해를 최소화하도록 하고 있다. 이와 함께 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 제정하여 민간분야의 개인정보보호를 지원하도록 하고 있다. 개인정보를 얻고자 하는 경우 일정한 약관을 통해 이용자의 동의를 받아야 하며, 영리 또는 부정한 목적으로 개인정보를 제공받지 못한다. 국내의 개인정보보호 관련 법률들은 원칙적으로 목적이외의 사용을 금하고 있으며, 정보의 수집부터 파기까지 다루고 있다.

4.2 건강정보보호를 위한 법률

건강정보보호와 관련하여 크게 보건의료기본법과 의료법, 건강정보보호법으로 나눌 수 있다. 우선 보건의료기본법은 건강정보 소유주의 기본 권리와 건강정보의 2차이용에 대한 제한 이유를 언급하고 있다. 의료법에서는 전반적인 의료 행위와 관련한 법으로 개인건강정보의 사용과 관련하여 정보 소유주의 동의 없이 해당 정보를 사용할 수 없도록 하며, 이용할 수 있는 경우를 한정적으로 제시하고 있다. 마지막으로 건강정보보호법은 개인정보를 취급하는 기관이 건강정보보호위원회의 심의를 거치도록 하며, 통계 및 학술 연구를 위해 개인을 식별할 수 없는 형태로 제공하는 경우에 대해 허용하도록 규정되어 있다.

4.3 의료연구 및 기타 2차이용을 위한 법률

OECD의 프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인과 국제연합의 컴퓨터화된 개

11) 개인정보보호법 제2조, 제15조, 제16조, 제17조, 제18조
12) 유전자치료, 인간게놈 프로젝트 등 생식(세포)관련기술과 유전자 관련기술 등이 도입되면서 후생노동성과 문부과학성등을 중심으로 유전자치료임상연구에 관한 지침(2002), 인간게놈,유전자해석에 관한 윤리지침(2001)등을 발표하였다 .
13) 개인정보보호법 제21조

인정보파일의 규율에 관한 가이드라인, EU가 제정한 개인정보의 처리 및 자유로운 전송에 관한 개인정보지침 등의 국제 규범을 포괄하고 있는 개인정보자기결정권은 현재 우리나라의 기본권으로 인정하고 있다. 이외의 헌법상의 자유와 관련된 권리 등이 있으며, 개인건강정보가 개인정보의 일부임으로 개인건강정보를 2차적으로 이용하는 부분에 있어서 적용할 수 있다.

V. 국내외 개인건강정보의 2차이용 관련 법률 비교 및 검토

앞 절에서 IT기술과 의료서비스의 결합으로 축적, 공유되는 개인건강정보가 의학 분야 연구와 발전을 위해, 그리고 의료서비스의 질을 향상시키기 위해 2차적으로 사용될 때 개인의 프라이버시를 보호할 수 있도록 각국이 제정하고 요구하고 있는 법안들을 살펴보았다. 본 절에서는 앞에서 다룬 법안들의 비교 분석을 통해 앞으로 개인의 프라이버시를 존중하고 더불어 의료서비스의 발전을 도모할 수 있는 방향을 제시하고자 한다.

5.1 국내외 개인건강정보의 2차이용 관련 법률 비교 및 검토

대부분의 나라들은 개인정보에 대한 법안 속에 개인건강정보에 대한 취급을 포함하여 다루고 있으며, 미국을 제외하고 개인건강정보의 2차적 이용에 대한 법이 별도로 제정되어있지 않은 실정이다. 또한 미국과 영국은 개인의 민감한 정보에 대하여 이름, 주소, 나이, 과거병력 등 세부적으로 항목을 나누어 제시하는 반면 한국과 일본은 민감한 정보라고 하여 일반화하고 있다. 한편, 정보의 주체인 환자의 사전 동의에 대해서는 모든 나라에서 법으로 정의하고 있으며, 2차 이용과 관련하여 그 목적을 심사, 승인 및 감독 업무를 수행하는 기관이 미국은 PHDSC, 영국은 의학연구위원회, 일본은 국민보험조합, 한국은 건강정보보호위원회로 비교 국가 모두 가지고 있다.

2차 이용관련 사용목적의 사전 공지 및 공표와 관련하여 영국은 매우 엄격한 잣대를 가지고 있으며, 미국과 일본도 이와 관련된 법률을 존재하나, 한국에서는 별도의 공지나 공개와 관련한 법률을 가지고 있지 않다. 또한 2차적 이용 목적과 관련된 정보만을 제공받는 것에 대해 대부분의 나라가 관련 법률을 제정하고 있으나, 2차적 이용을 위해 제공받은 정보에 대한 접근에 대해서는 한국과 일본의 경우 별도의 법이 제정되어 있지 않다. 다행히 제공받은 정보에 대한 기밀성은 모든 나라에서 법으로 제정하고 있다. 하지만 연구의 자율을 보다 권장하는 영국의 경우는 정보의 무결성에 대한 법률이 부재하며, 일본의 경우도 이와 관련하여 별도의 언급이 없다. 그러나 미국과 한국의 경우 무결성을 갖출 것을 명시하고 있다.([표4]참조)

5.2 각 보안요구사항의 분석 및 역할

유헬스 시대의 도래와 함께 보다 나은 의료서비스를 제공하기 위해 의료기관 뿐 아니라 연구기관, 유관기관 및 정보통신 업체 등에 의해 개인건강정보는 2차적으로 이용될 수밖에 없다. 이는 곧 환자의 개인건강정보가 노출될 수 있다는 것을 뜻하고 보다 나은 의료 서비스를 제공받기 위해 개인정보의 공개를 감수해야 한다는 말이다[9]. 하지만 개인의 민감한 정보를 포함하고 있는 개인건강정보가 별다른 대책 없이 제2의, 제3의 기관에서 사용된다면 개인의 프라이버시의 침해를 초래할 수 있고, 궁극적으로 의료서비스의 개발 및 연구에 지장이 생길 수밖에 없다. 미국 등 선진국과 함께 국내에서도 정보화 수준의 향상과 정보보호의 관심이 높아지고는 있지만 많은 노력을 기울이지 못하고 있는 것이 현실이다. 따라서 의료기관을 포함하여 관련 정부기관 및 개인건강정보를 취급하는 모든 기관들의 의식제고와 체계적이고 종합적인 노력이 필요하다.

본 절에서는 개인건강정보의 주체와 2차 사용자, 그리고 중앙기관으로 나누어 각 보안요구사항에 맞는 역할을 제시하고자 한다.

5.2.1 개인건강정보의 주체

개인건강정보의 주체는 의료데이터를 생성하며 정보노출 등으로 인한 피해와 직접적인 관련이 있다. 따라서 개인건강정보의 주체는 반드시 자신의 건강정보가 보호되도록 관심을 기울이고, 적극적으로 의사표현을 해야 한다. 특히 모든 법률에서 환자의 동의를 반드시 받게 되어 있기 때문에 이를 통해 최소한의 피해가 일어나도록 예방할 수 있다.

5.2.2 개인건강정보의 2차 사용자

개인건강정보의 2차 사용자는 목적과 역할에 맞는

데이터를 전달받아야 하며, 전달받은 데이터를 안전하게 관리, 보존해야 한다. 따라서 다음과 같은 역할이 요구된다.

- ○ 개인건강정보의 열람 시 정보주체에게 통지 및 동의를 구해야 한다.
- ○ 개인건강정보를 2차이용을 위해 전달받은 데이터를 안전하게 관리, 보존해야 하며, 다음의 보안요구사항을 보장하기 위해 적절한 대응책을 준비해야 하며, 해당 직무에 대한 매뉴얼을 가지고 수행해야 한다.
  - 기밀성(Confidentiality)
    : 익명성보장(Anonymity), 연결불가능성(Unlinkability), 식별 불가능성(De-identification)을 보장해야 하며, 데이터의 암호화(Cryptography)를 수행해야 한다.
  - 무결성(Integrity)
    : 읽기(Read), 쓰기(Write), 수정(Modify), 삭제(Delete) 및 검색(Search) 등 데이터의 관리 필요, 전자서명, 데이터 관리 로그 등을 사용해야 한다.
  - 가용성(Availability) 및 접근 제어 (Access control)
    : 해당목적에 맞는 필요한 데이터만을 요청, 전달, 데이터 접근 로그 관리, 외부로부터의 보호를 위해 침입차단시스템, 침입탐지시스템, 방화벽을 운영, 데이터의 백업을 실시해야 한다.

5.2.3 개인건강정보의 중앙관리기관

중앙관리기관은 개인건강정보가 안전하게 전달되고 관리되며 사용되어 의료분야의 발전과 함께 질 높은 의료서비스를 받을 수 있는 역할을 해야 한다. 하지만 아직 개인건강정보에 대한 세부적인 정의와 각 정보의 노출위험에 따른 피해나 프라이버시 침해에 대해 제정된 바가 없다. 따라서 우선적으로 개인 건강정보에 대해 노출 시 발생할 수 있는 프라이버시 피해 정도에 따른 세부적인 정의가 필요하며, 이에 대한 연구도 수행돼야 할 것이다. 또한 효율적인 상호교환과 관리를 위해 관련 표준들을 제정하여야 할 것이다. 이는 개인건강정보가 공중보건 및 의료분야 연구, 의료 서비스의 개발 등을 위해 2차적으로 사용될 때 최대한 개인의 프라이버시를 침해하지 않도록 개인건강정보의 기준을 명확히 하는 것으로 관련 기관의 이해를 돕고 효율적으로 적절한 정보의 공유를 통한 연구와 서비스 발전이 일어날 수 있도록 기초를 마련할 것이다.

또한 개인건강정보의 2차이용에 초점을 맞춘 법제도의 정비가 필요할 것이다. 법제도, 승인 및 인증제도 등을 도입하여 개인건강정보에 대한 강제적인 조치를 통해 개인의 프라이버시를 최대한 보장하도록 하여 의료서비스의 질 향상과 의료분야의 연구에 안전하게 사용될 수 있도록 해야 한다. 또한 의료기관 등 개인건강정보 2차이용에 대해 별도의 승인과 감독과정을 강화하여, 본래의 목적이외에 개인건강정보가 사용되는 것을 사전에 방지할 필요가 있다.

마지막으로 개인건강정보를 다루는 관련 모든 기관들의 정보보호 의식 제고가 필요하다. 의료 기관 등 개인건강정보를 취급하는 기관들이 관련 법률이나 보안 표준들을 실질적으로 준수, 수행하여야 여러 제도나, 법적인 노력이 의미가 있다. 따라서 관련 모든 기관들이 개인건강정보보호에 대해 숙지할 수 있도록 교육과 훈련을 실시하는 등 개인건강정보보호가 효과적으로 수행되도록 해야 할 것이다.

VI. 결 론

IT기술을 활용한 의료서비스의 발전은 유헬스와 같은 새로운 개념의 의료서비스를 제공, 지원가능하게 했다. 이와 더불어 전자화된 개인건강정보는 접근과 관리 및 검색이 용이하여 보다 나은 의료 서비스를 제공하기 위해 의료분야의 연구나 공중보건의 증진을 목적으로 2차적으로 이용, 활용되는 추세이다. 하지만 부주의하게 개인의 건강정보를 이용하는 경우 환자 개인의 프라이버시 손상이 발생할 수 있고, 이는 의료분야의 연구 등에 개인건강정보가 2차적으로 이용되는데 걸림돌로 작용하여 2차이용을 통한 의료서비스의 발전과 연구에 제한이 발생할 수 있게 된다. 하지만 아직 개인건강정보를 이용한 2차적 이용에 대해 체계적인 연구나 논의가 없는 것이 현실이다. 따라서 본 논문에서는 개인건강정보의 2차이용과 관련하여 국내외의 법안들을 살펴보고 이를 비교 분석하였다. 앞으로 개인의 프라이버시를 존중하고 더불어 의료서비스의 발전을 도모할 수 있도록 개인건강정보에 대한 세부적인 정의와 관련 표준들의 정의, 관련 법제도의 정비와 감독의 강화가 있어야 할 것이다. 또한 관련 기관들의 개인건강정보 취급에 있어 정보보호 의식의 제고도 필요할 것이다.

참고문헌

[1] 김홍근, 김윤정, 지식정보사회 의료 패러다임 변화와 정보보안, 정보보호 정책동향 정책개발06-05, 한국인터넷진흥원, 2006년 5월

[2] Secondary uses and re-use of healthcare data : taxonomy for policy formulation and planning, AMIA, 2007년

[3] 송지은, 김신효, 정명애, 정교일, "u-헬스케어 서비스에서의 의료정보보호," 한국정보보호학회, 정보보호학회지, 17(1), pp.47-56, 2007년 2월

[4] 송유진, 박광용, "의료데이터 공유 및 활용서비스를 위한 보안/프라이버시 요구사항," 정보보호학회지, 20(3), pp.90-96. 2010년 3월

[5] HIPPA, http://www.hhs.gov/ocr/hippa

[6] PHDSC, http://www.phdsc.org

[7] MRC(Medical research council ethics serises), http://www.mrc.ac.uk

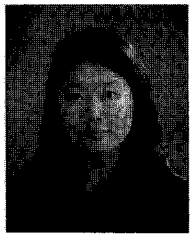
[8] EHR 핵심공통기술 연구개발 사업단, 건강정보보호 및 보안체계개발보고서, EHR 핵심공통기술 연구개발 사업단, 2010년 3월

[9] 박우성, 개인정보보호 의료기관 개인건강정보보호, Pacific books, 2010년

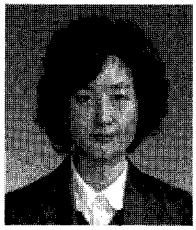
[10] 김동수, 김민수, "e-health 시대의 진전에 따른 의료정보보호 쟁점 및 정책방향," 정보화정책, 13(4), pp.128-148, 2006년

[11] 정혜정, 김남현, " u-Health 시대의 개인건강정보보호를 위한 관련 법제 고찰," 정보보호학회논문지, 19(1), pp.115-124. 2009년 2월

〈著者紹介〉



박 한 나(Han-na Park) 정회원
2008년 2월: 서울시립대 수학과 학사
2010년 2월: 고려대학교 정보보호학과 석사
2010년 9월 ~ 현재: 한국전자통신연구원, 연구원
〈관심분야〉 RFID/USN, 정보보호, 유헬스, 프라이버시보호



정 부 금(Boo-Geum Jung) 정회원
1986년 2월: 부산대학교 계산통계학과 학사
1991년 8월: 숙명여자대학교 전산학과 석사
1986년 1월 ~ 현재: 한국전자통신연구원 책임연구원
〈관심분야〉 Security, 프라이버시보호, Internet Platform/Operating System /Distributed Network

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 학사
1987년 12월: Oklahoma University 전산학과 석사
1992년 5월: Oklahoma University 전산학과 박사
1993년 3월 ~ 1997년2월: 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년2월: 고려대학교 전산학과 부교수
2001년 2월 ~ 현재: 고려대학교 정보경영공학전문 대학원 교수
〈관심분야〉 암호프로토콜, RFID/USN 보안, 프라이버시보호기술

정 교 일(Kyo-Il Chung) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 8월: 한양대학교 대학원 전자계산학과 석사
1997년 8월 한양대학교 대학원 전자공학과 박사
1980년 12월 ~ 1981년 11월: 엠-시스템즈 연구원
1981년 12월 ~ 1982년 2월: 한국전기통신연구소 위촉연구원
1982년 3월 ~ 현재: 한국자통신연구원 책임연구원
1984년 1월 ~ 현재: 대한전자공학회 표준화 상임이사, 평의원
〈관심분야〉 RFID/USN, 정보보호, IT-융합(국방, 유헬스, 방재 등)