환자 의료정보 보호의 문제

정 부 균 *

*논문접수: 2008. 10. 20. *심사개시: 2008. 11. 20. *게재확정: 2008. 12. 14.
*삼성의료원 법무실 과장

I. 서 론

2008년은 개인정보 수난의 해라고 할 수 있다. 유난히도 크고 광범위한 개인정보가 침해되는 사건들이 발생했었다. 2008년 2월에는 옥션의 해킹으로 1,081만명의 개인정보 유출되었고, 4월에는 하나로텔레콤이 회원의 동의 없이 텔레마케팅 등에 고객정보를 유용했다. 5월에는 미국인 해커가 총 274개 기관 전산망을 해킹해서 고객정보 970만건을 유출했다. GS칼텍스의 정보유출은 해킹이 아니라 내부자의 의도적 유출이라는 점에서 더욱 충격적이며 유출 규모도 국내 성인인구에 맞먹는 1125만 명이라는 점도 그렇다. 또한 GS 칼텍스 사건은 기업의 보안 시스템이 얼마 허술한지를 보여주는 사건이기도하다. 국민건강보험공단이나 LG 데이콤, 다음의 정보유출도 있었다. 2008년에 개인정보유출 사건이 유독이 많았던 이유는 그동안의 위험한 상황이 현실로 나타났음에 다름이 아니라고 생각한다. 즉, 지금까지 누적된 위험이 한꺼번에 튀어나온 것이다. 그렇다면 이러한 시점이 개인정보 보호를 위한 제도적 기술적 조치를 강구해야 할 때라고 생각한다.

국민건강보험공단 직원이 개인정보 12,033건을 불법으로 열람하고, 1,855건의 개인 의료정보를 유출한 사건은 비단 일반적 개인정보만이 아니라 의료정보 역시 심각한 위험에 노출되어 있음을 보여주는 것이다. 정보통신 기술을 비롯한 과학기술과 의료기술의 비약적인 발전은 국민 삶의 질적 향상과 함께 의료서비스에 대한 관심을 증폭시키고 있다. 또한 국내 의료기관들의 경쟁력 향상노력이 계속되고 있는 가운데 의료정보화는 이제 병원정보화와 e-Health[1]를 거쳐 u-Health[2]로의 진행을 가속화하고 있다.

---

1) e-Health는 정보통신기술을 이용하여 최대한 의학지식과 환자정보를 제공함으로써 환자진료 및 개인건강관리 시에 효율적이고 합리적인 의사결정을 지원할 수 있는 정보체계임(보건복지부 정의). e-Health의 대표적 서비스인 원격의료는 의료인의 효율적 시간활용, 신속하고 편리한 진료의뢰, 지속적 진료, 자료공유 등의 장점으로 90년대 중반이후 시범사업을 추진해 오고 있으나 활성화되지 않고 있다.

2) u-Health는 ubiquitous Health의 약자로, 정보기술과 보건의료를 결합하여 언제 어디서나 환자의 질병에 대한 예방·진단·사후관리 등 보건의료 서비스를 제공하는 것을 의

의료정보화는 환자 원무기록의 디지털화, 영상정보 저장기록화, 병원업무전산화 등 병원정보화 단계가 진행 중에 있고 인터넷이나 무선기기를 이용한 원격의료[3] 등이 현실화 되고 있는 단계이며, 일부 병원에서는 센서를 이용한 의료정보의 획득과 상시접근을 통한 유비쿼터스의 개념이 실현되어 가고 있다[4][5].

이러한 의료정보화 분야의 급속한 발전으로 환자들은 보다 업그레이드된 의료서비스를 누릴 수 있게 되었다. 그러나 다른 정보화 분야에서와 마찬가지로 정보화 역기능을 제대로 예방, 대응하지 못할 경우 다른 분야보다 훨씬 심각한 보안위협 가능성이 나타날 수 있다. 개인의 의료정보가 적절히 관리되지 않아 유출될 경우 개인정보의 침해는 다른 정보의 유출보다 훨씬 심각할 것으로 예상된다[6].

따라서 이하에서는 개인정보에 대하여 개념과 침해 및 보호의 문제를 개략적으로 검토 해 보고, 개인정보의 특별한 한 형태로 이해할 수 있는 의료정보의 보호 문제를 다양하게 검토해 보기로 한다. 특히 의료가 IT 기술의 발달에 힘입어 더욱 발전해 가고 있으며 그에 따른 정보보안의 문제도 더욱 복잡하고 심각해지고 있다는 점에 무게중심을 두고 검토해 보고자 한다.

미한다. e-Health와 u-Health에 대해서 보다 상세한 내용은, 한국정보보호진흥원,『유비쿼터스 환경에서의 정보보호 정책 방향』, 지식경제부, 2008. : 한국정보보호진흥원,『원격 의료용 바이오 인증 기술 및 표준개발』 참조.

3) 2002년 의료법 개정 시 원격의료 및 전자의무기록 관련 규정을 도입하였다.

4) 김홍근·김윤정,『지식정보사회 의료 패러다임 변화와 정보보안』, 한국정보보호진흥원, 2006, 1-5면.

5) LG CNS에서는 인텔과 공동으로 신개념 홈헬스케어 서비스 '터치닥터'를 출시하고 2008년 4분기부터 상용 서비스를 제공할 계획이다. 이 서비스는 고혈압이나 당뇨환자들이 '터치닥터' 단말기를 구입하고 집에서 혈압 등 자신의 건강 수치 및 생활 습과 상태를 스스로 측정하고, 이 데이터는 전문 상담사가 상주하는 건강관리센터에 보내져 실시간으로 분석된다. 이 자료는 종합병원의 전문 의료진에게도 전송 되 환자와 담당의사가 전화·인터넷·동영상 상담이 이루어지는 개념이다.(매일경제, 2008.8.29.) 이러한 서비스는 유비쿼터스를 기반으로 한 U-Health 시대가 본격적으로 개막되고 있다는 것이다.

6) 환자의 의식 변화에 대해서는, 유지원,「진료정보의 개인정보보호에 대한 의료인과 환자의 인식도 비교」, 석사학위논문, 고려대보건대학원, 2006, 9-14면 참조.

II. 개인 정보

1. 개인정보의 의의

가. 개인정보의 개념

개인정보는 “개인”과 “정보”라는 두 단어로 이루어진 복합명사이다. 여러 가지 정보중 개인과 관련된 정보를 의미하는 것으로 이해할 수 있다. 우선 정보의 사전적 의미를 보면 백과사전에서는 “생활 주체와 외부의 객체 간의 사정이나 정황(情況)에 관한 보고”[7]라고 하며, 국어사전에서는 “관찰이나 측정을 통하여 수집한 자료를 실제 문제에 도움이 될 수 있도록 정리한 지식. 또는 그 자료”[8]라고 설명하고 있다. 사전적 의미의 핵심은 ‘자료’라고 할 것이다.

개인정보라고 할 때 “개인”에 대한 해석이 달라질 수 있는데 대개 두 가지 개념으로 나누어지고 있다고 한다[9]. 하나는 ‘개인’정보를 “개인적” 정보로 이해하려는 의견이다. 이 때 ‘개인적’이라는 말은 “사적인”과 같은 의미로 이해될 수 있으며, 개인정보는 사적정보 또는 사적영역의 정보와 같은 의미로 사용될 수 있다. 이때의 의미는 공적인 성격을 띠는 정보가 아니라는 의미로 이해된다.

또 다른 하나는 개인정보를 “개인에 관한”정보로 이해하려는 의견이다[10]. 개인과 관련되는 신상에 관한 사항들을 개인정보로 파악하는 것인데, 정보의 주체에 주목한 개념이라고 할 수 있다. 이 때는 정보의 공적·사적 성격을 묻지 않고 개인에 관련된 정보 일체를 의미하게 된다.

개인정보를 ‘사적인 정보’로 볼 것인지, ‘개인에 관한 정보’로 볼 것인지

---

7) 두산백과사전, 인터넷 네이버 검색.
8) 국어사전, 인터넷 네이버 검색.
9) 권건보, 『개인정보보호와 자기정보통제권』, 경인문화사, 2005, 9면.
10) ‘개인’의 의미를 ‘사적인’ 것과 ‘개인에 관한’ 것이라는 두 가지 의견에 대한 상세 내용은, 권건보, 전게서, 9-11면 참조.

양자의 차이는 고전적인 '프라이버시'[11]와의 관계성에 있다. 즉, 사적인 정보로 이해하는 경우 고전적인 프라이버시와 관련성이 높을 것이며, 개인에 관한 정보로 이해하는 경우 고전적인 프라이버시보다는 개인의 자율성, 인격성의 관점에서 보게 된다는 차이가 있다. 현대 사회에서 보호의 대상이 되는 개인정보는 '사적인 정보'라는 측면보다는 '개인에 관한 정보'로 이해하는 것이 바람직하다는 의견이 일반적이다[12].

나. 법률상 개인정보의 개념

'정보통신망이용촉진및정보보호등에관한법률'(2001.7.1.시행) 제2조 제1항 제6호에 의하면, 개인정보란 "생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성 · 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다."고 규정하고 있다.

'공공기관의개인정보보호에관한법률' 제2조 제2호에서는 개인정보라 함은 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명 · 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다."고 규정하고 있다. 이러한 개인정보의 개념은 개인의 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실 · 판단 · 평가를 나타내는 일체의 정보가 포함되는데, 이는 개인식별

---

11) 프라이버시(privacy)는 라틴어로 '떼어놓다', '격리시키다'라는 의미를 가진 private의 명사형이다. 영어사전에서는 개인의 비밀이라는 의미로 설명되고 있다. 역사적인 발전과정에서 프라이버시권은 '홀로 있을 수 있는 권리'라는 소극적인 의미로 이해되고 있었으나, 최근에는 자기정보 내지 개인정보에 관한 정보의 흐름을 통제하는 개인의 적극적인 권리의 의미로 이해되고 있다. 프라이버시 및 프라이버시권과 헌법상 프라이버시권의 형성 과정 등에 대한 상세 내용은, 백윤철 · 이창범 · 장교식, 『개인정보 보호법』, 한국학술정보, 2008, 158-162면 참조.

12) 권건보, 전게서, 12면.

〈표 1〉 개인정보의 유형과 종류

구 분	개인정보의 종류
일반 정보	이름, 주민등록번호, 운전면허번호, 주소, 전화번호, 생년원일, 출생지, 본적지, 성별, 국적
가족 정보	가족 구성들의 이름, 출생지, 생년월일, 주민등록번호, 직업, 전화번호
교육 및 훈련정보	학교출석사항, 최종학력, 학교성적, 기술자격증 및 전문 면허증, 이수한 훈련프로그램, 동아리활동, 상벌사항
병역 정보	군번 및 계급, 제대 유형, 주특기, 근무부대
부동산 정보	소유 주택, 토지, 자동차, 기타 소유 차량, 상점, 건물 등
동산 정보	보유 현금, 저축현황, 현금카드, 주식, 채권 및 기타 유가증권, 수집품, 고가의 예술품, 보석
소득 정보	현재 봉급액, 봉급 경력, 보너스 및 수수료, 기타 소득의 원천, 이자소득, 사업소득
기타 수익정보	보험(건강, 생명 등) 가입 현황, 회사의 판공비, 투자 프로그램, 퇴직 프로그램, 휴가, 병가
신용 정보	대부 잔액 및 지불상황, 저당, 신용카드, 지불연기 및 미납의 수, 입금 압류 통보에 대한 기록
고용 정보	현재의 고용주, 회사주소, 상급자의 이름, 직무수행 평가기록, 훈련기록, 출석기록, 상벌기록, 성격 테스트 결과, 직무태도
법적 정보	전과기록, 자동차 교통위반기록, 파산 및 담보기록, 구속기록, 이혼기록, 납세기록
의료 정보	가족병력기록, 과거의 의료기록, 정신질환기록, 신체장애, 혈액형, IQ, 약물 테스트 등 각종 신체 테스트 정보
조직 정보	노조가입, 종교단체 가입, 정당 가입, 클럽 회원
통신 정보	전자우편, 전화 통화 내용, 로그파일(log file),쿠키(cookies)
위치 정보	GPS나 휴대폰에 의한 개인의 위치정보
신체 정보	지문, 홍채, DNA, 신장, 가슴둘레 등
습관 및 취미 정보	흡연, 음주량, 선호하는 스포츠 및 오락, 여가 활동, 비디오 대여기록, 도박 성향 등

이 가능한 정보로는 내면의 비밀(사상, 신조, 종교, 가치관, 양심 등)과 심신의 상태(체력, 건강상태, 신체적 특징, 병력 등), 사회경력(학력, 범죄경

력, 직업, 자격, 소속정당 · 단체 등), 경제관계(재산상황, 소득, 채권채무 관계 등), 생활 · 가정 · 신분관계(성명, 주소, 본적, 가족관계, 출생지, 본관 등) 등으로 구체화 될 수 있다[13].

'전자서명법' 제2조 제13호에서는 "생존하고 있는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 · 영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"고 규정하고 있어 각 법률에서 개인정보는 거의 동일한 의미로 정의되고 있음을 알 수있다. 일반적으로 말하면, 본인의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 정보주체(혹은 당사자)의 안녕과 이해관계에 영향을 미칠 수 있는 개인관련 정보는 모두 개인정보(personal information)라고 할 수 있다[14].

다. 개인정보의 유형과 종류

개인정보의 유형과 종류를 구분하는데 정형화된 것은 없고 학자들마다 차이가 있지만 대개 〈표 1〉과 같이 정리해 볼 수 있다[15].

라. 개인정보의 등급

정부나 기업이 개인정보보호 정책을 수립하는 데 있어 개인정보의 유형에 못지않게 중요한 것이 개인정보의 등급인데 아직 법제화 되지는 않았다. 그렇지만 개인정보에 대한 보호가 강화되면서 개인정보의 내용에 따라 등급을 구분하는 것이 필요하게 되었다. 일반적인 정보에 있어서도 비밀 취급 등의 등급이 있는 것처럼 개인정보의 민감도에 따라서 5등급으로

---

13) 총무처, 『축조해설 개인정보보호법』, 1994, 31면 : 권건보, 전게서, 17면에서 재인용.
14) 한국정보보호진흥원, 『개인정보보호백서』, 2002, 25면.
15) 권건보, 전게서, 18-20면 참조 : 한국정보보호진흥원, 전게서, 26면 참조.

〈표 2〉 개인정보의 등급

등 급	개인정보의 유형
1급 개인정보	신조·의료·성생활·인종·혈통·범죄·국가안보와 관련된 비밀정보 등
2급 개인정보	교육·고용·금융신용·주민번호·자격증명·지문·혈액형·DNA·출입국정보 등
3급 개인정보	개인이 제출한 정보, 프로파일 된 개인정보, 법령에 의한 수집정보 등
4급 개인정보	기관의 견해, 타인의 견해, 정보구관의 응답, 공개가능한 통신문 등
5급 개인정보	연구목적, 통계목적, 학술자료 등의 집합적으로 활용되는 정보

분류 해 보는 의견이 있으며 〈표 2〉와 같다[16].

2. 개인정보의 침해

가. 개인정보 침해 유형

개인정보가 침해되는 유형은 여러 가지로 구분 해 볼 수 있지만 크게 6가지로 구분해서 설명하는 견해가 있다[17]. 즉, ① 부적절한 접근과 수집, ② 부적절한 모니터링 ③ 부적절한 분석, ④ 부적절한 이전 ⑤ 원하지 않는 영업행위 ⑥부적절한 저장으로 구분하여 설명한다.

또 다른 견해로는 ① 명의도용에 따른 신용사기로 인한 재정적 피해, ② 명의를 도용한 자가 행한 명예훼손, 모욕 등으로 인해 형사사건의 혐의자가 되거나, ③ 수집된 개인정보가 부정확 부적정한 경우 개인정보 주체에 대한 그릇된 판단을 초래해 신용 및 명예훼손 초래, ④ 지속적인 개인정보 수집으로 인한 사생활 감시로 불유쾌 및 불편이 초래되거나 사회적 활동에 지장을 초래, ⑤ 원하지 않는 광고성 정보 등의 수신으로 인한 생활의 평온 파괴, ⑥ 생명, 신체상의 위해 가능성 등으로 구분해서 설명한다[18].

---

16) 윤영민·정영화·이헌수, "안전한 전자정부를 구현하기 위한 개인정보보호 및 정보보안 대책", 전자정부특별위원회, 2002. : 한국정보보호진흥원, 전게서, 27면에서 재인용.
17) 한국정보보호진흥원, 전게서, 29-31면.

〈표 3〉 개인정보 침해 유형 분류표

No	침해 유형	법률 근거
1	이용자 동의 없는 개인정보 수집	정보통신망법 제22조 제1항
2	개인정보수집시 고지 또는 명시의무 불이행	정보통신망법 제22조 제2항
3	과도한 개인정보 수집	정보통신망법 제23조
4	이용자 동의 없는 개인정보 목적 외 이용 또는 제3자 제공	정보통신망법 제24조 제1항
5	개인정보취급자에 의한 훼손 · 침해 또는 누설	정보통신망법 제24조 제4항
6	개인정보처리 위탁시 고지의무 불이행	정보통신망법 제25조 제1항
7	영업의 양수 등의 통지의무 불이행	정보통신망법 제26조 제1항
8	개인정보관리책임자 미지정	정보통신망법 제27조 제1항
9	개인정보보호 기술적 · 관리적 조치 미비	정보통신망법 제28조
10	수집 또는 제공받은 목적 달성 후 개인정보 미파기	정보통신망법 제29조
11	동의철회 · 열람 또는 정정 요구 등 불응	정보통신망법 제30조 제1항 및 제2항
12	개인정보 오류정정요구 접수 후 미 정정 정보이용	정보통신망법 제30조 제5항
13	동의철회 · 열람 · 정정을 수집방법보다 쉽게 해야 할 조치 미 이행	정보통신망법 제30조 제6항
14	법정대리인의 동의 없는 아동의 개인정보 수집	정보통신망법 제31조 제1항
15	타인정보의 훼손 · 침해 · 도용	
16	기타 (신용정보침해, 직장 프라이버시 침해 등)	

한편 '개인정보 분쟁조정위원회'에서는 정보통신망이용촉진및정보보호등에관한법률의 규정에 따라 다음 〈표 3〉과 같이 개인정보침해유형을 분류하고 있다[19].

18) 한국정보보호진흥원, 전게서, 60면.

19) 강달천 외 2인, 『2005년 개인정보 피해구제 및 상담사례분석』, 한국정보보호진흥원, 2005, 42면.

〈표 4〉 침해 유형별 신청 현황

침해 유형	건수	비율
이용자 동의 없는 개인정보 수집	1,140	6.3
개인정보 수집시 고지 또는 명시의무 불이행	15	0.1
과도한 개인정보 수집	33	0.2
고지 · 명시한 범위를 초과한 목적 외 이용 또는 제3자 제공	916	5.0
개인정보 취급자에 의한 훼손 · 침해 또는 누설	186	1.0
개인정보 처리 위탁 시 고지의무 불이행	4	0.05
영업의 양수 등의 통지의무 불이행	7	0.05
개인정보관리책임자 미 지정	25	0.2
개인정보보호 기술적 · 관리적 조치 미비	390	2.1
수집 또는 제공받은 목적 달성 후 개인정보 미파기	152	0.8
동의철회 · 열람 또는 정정 요구 등 불응	771	4.2
동의철회 · 열람 · 정정을 수집방법보다 쉽게 해야할 조치 미이행	285	1.6
법정대리인의 동의없는 아동의 개인정보 수집	71	0.4
주민번호 등 타인 정보의 훼손 · 침해 · 도욕	9,810	53.9
기타 (신용정보침해, 직장 프라이버시 침해 등)	4,401	24.1
합 계	18,206	100

나. 개인정보 침해 현황

한국정보보호진흥원의 '개인정보 분쟁조정위원회'에서 발표한 자료에 의하면 2005년 한 해 동안 개인정보가 침해되었다고 피해구제 및 상담신청을 한 현황은 〈표 4〉와 같다[20].

20) 강달천 외 2인, 위의 책, 36면.

3. 개인정보 보호

가. 개인정보 보호 방법

개인정보를 보호하는 가장 대표적인 방법이 입법에 의한 것이다. 입법방식으로는 ① 통합방식(omnibus 방식), ② 분할방식(segment 방식), ③ 개별방식으로 나눌 수 있다[21]. 통합방식은 공정부분과 민간부문을 하나의 법률에 의해 포괄적인 규제의 대상으로 하는 방식이고, 분할방식은 공적부문과 민간부문을 각각 별개의 법률에 의해 규제의 대상으로 하는 방식이며, 개별방식은 규제의 대상을 한정해서 개별영역 별로 규제를 하는 방식이다.

개인정보를 보호하기 위한 법률의 대부분은 '통합방식'을 취하고 있으며 한국과 일본도 이 방식을 취하고 있다.

나. 각국의 개인정보 보호동향[22]

(1) OECD 이사회의 가이드라인

국제기관에 의한 개인정보 보호 대응방법으로 지침 역할을 하고 있는 것이 경제협력개발기구(OECD)가 1980년 9월 23일에 채택한 '프라이버시 보호와 개인데이터의 국제유통에 관한 가이드라인에 대한 이사회권고'이다. OECD 권고는 개인정보 보호를 위해 8개의 원칙을 제시하였다. 즉, ① 수집제한의 원칙, ② 정보정확성의 원칙, ③ 목적명확화의 원칙, ④ 이용제한의 원칙, ⑤ 안전보호의 원칙, ⑥ 개인참가의 원칙, ⑦ 공개의 원칙, ⑧ 책임의 원칙 을 제시하고 있다[23].

---

21) 백윤철, "우리나라에서 의료정보와 개인정보보호", 『헌법학연구』, 제11권 제1호, 2005, 400면.

22) 백윤철, 전게논문, 400-409면 참조.

23) OECD 가이드라인 8원칙의 상세한 내용은, 백윤철, 전게논문, 401-402면 참조.

(2) 유럽평의회의 개인데이터 보호조약

OECD 가이드라인 이후 유럽평의회에서 인준한 조약으로서, 권고가 아니라 조약이므로 유럽에서는 OECD 가이드라인보다 가맹국에 대한 구속력이 강하다. 주요내용은 ① 데이터의 취득 및 처리의 공정함, ② 합법적인 목적에서의 이용과 축적, ③ 개인정보의 처리목적이 적절할 것과 목적 이외로 정보처리하지 않을 것, ④ 정보의 정확성 및 갱신, ⑤ 필요기간을 넘긴 데이터 축적의 금지 등에 대해서 규정하고 있다.

(3) EU의 개인데이터 보호지침

1995년 10월 24일 유럽의회 및 이사회는 '개인데이터 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 지침'을 채택하였다. 이 지침은 자동처리 및 수동 처리된 개인데이터의 처리에 적용된다. 이 지침은 유럽연합의 15개 가맹국의 법정비를 촉구하고 있다.

(4) 미국

미국은 공적부문과 민간부문 모두를 대상으로 한 포괄적인 개인정보보호법은 없지만, 공적부문 중에서 연방정부가 가지고 있는 개인정보에 대해서는 1974년의 프라이버시법이 제정되어 있고, 주 단위에서도 개별 영역마다 프라이버시 보호를 위한 법률이 제정되어 있다. 민간부문에 대해서는 자주규제를 원칙으로 하고 있으나 예외적으로 기밀성이 높은 정보를 다루는 분야에 있어서는 부문별로 프라이버시를 보호하는 개별법이 제정되어 있다.

(5) 일본

일본은 EU지침에서 정한 "적절한 개인정보보호 수준 확보"의 한 방안으로 일본 산업규격인 개인정보보호규격(JIS Q 15001)을 1999년 3월 제정하

〈표 5〉 개인정보 보호 관련 현행 법률

구분	관련법률	규제내용
정부기록정보	공공기관의 개인 정보 보호에 관한 법률	처리과정상의 정보주체 및 공공기관의 권리의무 규율
	공공기관의 정보 공개에 관한 법률	개인정보의 비공개, 부분 공개
	주민등록법	주민등록 열람 또는 등·초본교부, 전산자료 이용 등
	자동차관리법	자동차관리 업무의 전산처리시 사생활 보호
	통계법	통계작성 과정 시 개인 및 단체법인의 비밀 보호
	국정감사 및 조사에 관한 법률	사생활 침해 목적의 감사, 조사 제한
	국가공무원법	업무상 지득한 비밀의 보호
	독점규제 및 공정거래에 관한 법률	업무상 지득한 비밀의 보호
통신비밀	통신비밀보호법	우편물의 검열, 전기통신의 감청 등 통신관련 사생활 보호
	통신제한조치의허가절차및비밀유지에 관한규칙	범죄수사, 국가안보를 위한 통신제한 조치의 허가절차
	전기통신사업법	개별이용자에 관한 정보의 공개 및 유용금지 등
	형법 제316조 비밀 침해 죄	전자기록 등 특수매체기록에 대한 기술적 침해
보건의료정보	보건의료기본법	보건의료관련 사생활의 보호
	의료법, 전염병예방법, 후천성면역결핍증예방법, 장기이식등에관한법률, 정신보건법, 모자보건법, 응급의료에 관한 법률, 약사법, 형법(제317조 업무상 비밀 누설죄)	업무상비밀 누설 금지
	생명윤리 및 안전에 관한 법률	유전자정보의 보호 등
소비자정보	정보통신망 이용촉진 및 정보보호 등에 관한 법률	정보통신서비스 제공자 등에 의한 개인정보 취급 규제
	신용정보의이용및보호에관한법률	민간부분에 의한 개인신용정보 처리의 규제와 신용정보주체의 열람 및 정정 청구 등
	금융실명거래및비밀보장에관한법률	금융거래의 비밀보장
	증권거래법	정보의 제공, 누설 금지
	위치정보의이용및보호등에관한법률	위치정보의 수집·제공의 범위, 오·남용 방지
	은행법, 변호사법, 공증인법 등	업무상 지득한 비밀의 보호

였고, 2000년 10월 11일 '개인정보보호기본법제에 관한 대강'을 결정하고, 국회에서 통과되었다. 그 결과 개인정보보호의 기본을 정하는 개인정보보호기본법이 제정되어 2005년 4월부터 시행 되었다.

다. 현행법상 개인정보 보호

우리나라는 공적부문에서 '공공기관의 개인정보 보호에 관한 법률', '공공기관의 정보공개에 관한 법률' 및 '행정정보의 공동이용에 관한 규정' 등이 있으며, 민간부문에서는 '금융실명거래및비밀보장에관한긴급재정경제명령', '신용정보의 이용 및 보호에 관한 법률', '통신비밀보호법', '전기통신사업법', '정보화촉진법', '전자서명법', '전파법' 및 '정보통신망이용촉진및정보보호등에관한법률' 등이 각각 제정되어 시행되고 있다. 이러한 현행 법령을 표로 정리해 보면 다음 〈표 5〉와 같이 정리해 볼 수 있겠다.

III. 의료정보

1. 의료정보의 의의

'보건의료기본법' 제3조 제6호에서 "보건의료정보라 함은 보건의료와 관련한 지식 또는 부호 · 숫자 · 문자 · 음성 · 음향 및 영상 등으로 표현된 모든 종류의 자료를 말한다."고 규정하면서 동법 제3조 제1호에서 "보건의료라 함은 국민의 건강을 보호 · 증진하기 위하여 국가 · 지방자치단체 · 보건의료기관 또는 보건의료인 등이 행하는 모든 활동을 말하다."고 규정하고 있다.

의료정보의 개념에 대해서는 의무기록이나 진료카드를 거론하면서 이에 기록되는 내용(진료기록)이라는 견해가 있고[24], 이와 유사하게 진료정보

24) 이부하, "환자의 의료정보권", 『한양법학』, 제17집, 2005, 178면 이하 : 이인영, "개정

가 중심이 되면서, “의료제공의 필요성을 판단하거나, 또는 의료의 제공을 행하기 위하여 진료 등을 통해서 얻은 환자의 건강상태나 그들에 대한 평가 및 의료의 제공의 경과에 관한 정보”이고, 이것을 기록한 것이 진료기록이라고 하는 견해도 있다[25]. 후자와 같은 입장에서는 의료정보를 다음과 같이 구분할 수 있다고 한다[26].

① 환자의 기본정보 : 성명, 연령, 생년월일, 주소, 전화번호, 연락처, 근무지, 가족관계 등
② 건강보험과 복지정보 : 건강보험정보, 장애자 기록
③ 진료관리용 정보 : 진료정보, 적용보험정보, 내왕일자, 입 · 퇴원 등
④ 생활배경정보 : 흡연 여부, 음주 여부, 정신상태 여부
⑤ 의학적 배경정보 : 출생 시 체중, 임신 분만에 대한 진료기록, 예방접종에 대한 기록
⑥ 진료기록정보 : 진단, 진료계획, 현 병력 등
⑦ 지시실시기록정보 : 처방기록, 수술기록, 처치기록 등
⑧ 진료정보교환정보 : 진단서 등
⑨ 진료설명과 동의정보 : 각종설명정보, 각종동의정보
⑩ 요약정보 : 진료요약, 입원요약
⑪ 사망기록정보 : 사망진단서, 부검기록 등

이 견해는 의료정보는 특히 개인정보의 민감성, 의료행위의 전문성, 사회적 공익성을 갖고 있고, 이는 명백한 개인정보로서 의료행위에 의해 취득되는 전문성과 공익성을 강조하는 입장이다[27].

그런데 이와 같은 견해는 형식적 의미의 의료정보라고 볼 수 있는데, 의

의료법의 환자의 개인정보 보호규정에 관한 법리적 고찰”, 『한림법학 Forum』, 제11권, 2002, 138면 이하.

25) 김상찬, “의료정보의 제공에 관한 연구”, 『일감법학』, 제8권, 2003, 2002면 이하.

26) 백윤철, 전게논문, 417면, 주38.

27) 전영주, “의료정보와 개인정보보호”, 『법학연구』, 제23집, 523면 주2 : 길준규, “의료정보상 개인정보보호방안”, 『법과 정책연구』, 제6집 제1호, 123면.

료법시행규칙 제18조에서 규정하고 있는 환자명부, 진료기록부, 처방전, 수술기록부 등의 실질적인 진료기록을 의미하는 것이고, 기록된 내용 모두를 의료정보로 보기는 어려워 보인다며 비판하는 의견도 있다[28].

의료정보의 의의를 한마디로 정의하기는 어렵지만 간단히 의료정보를 정의 한다면 "진료를 받는 환자를 통해서 의료인이나 의료기관이 취득 · 보유하는 개인정보"라고 할 수 있을 것이다[29].

의료정보를 분류하면 주관정보, 객관정보, 가치판단정보로 분류될 수 있다[30]. 주관정보는 정보의 주체인 환자에 의해 발생하는 것으로서 환자에 의해서 기록되는 문서이므로 적절한 방식으로 작성 및 수정되어야 하고, 정당한 사유 없이 개인 의료정보가 탐지되거나 유출, 변조되거나 하면 안 된다. 객관정보는 검사, 진료 등의 정보이며, 가치판단정보는 의료종사자의 전문성에 기초하여 작성된 정보를 말한다. 가치판단정보는 '2차 전문의료정보' 또는 '가공의료정보'로 표현되기도 한다.

2. 타 개념과 구분

가. 생체정보

생체정보(Biometric Information)는 "개인의 고유한 특성으로부터 얻어지는 정보"라고 정의할 수 있고, 좁게는 신체적 특성, 넓게는 행동적 특성에서 얻어진다고 한다[31]. 이러한 생체정보는 의료서비스를 전제로 하지 않는 신체의 일부 그 자체에서 얻어지는 정보라고 할 수 있으므로 의료정보와 생체정보는 구분되어야 한다고 한다[32].

---

28) 길준규, 전게논문, 123면.
29) 장석천, "의료정보보호와 민사법적 문제", 『법학연구』, 제28집, 2007, 162면.
30) 상세한 내용은, 전영주, 전게논문, 526면 참조.
31) 이창범, "생체프라이버시보호 원칙에 관한 연구", 『인터넷법률』, 제31호, 2005, 20면.
32) 길준규, 전게논문, 125면.

나. 유전정보

의료정보와 유전정보를 구분할 수 있을 것인가. 생명공학의 눈부신 발전과 함께 부각된 인간의 유전정보는 유전자 진단과 치료라는 의학분야만이 아니라 임상연구와 실험에서 더 발전하고 있으며, 또한 범죄수사와 친자관계 확인, 인류학과 고고학 등 그 활용대상범위를 점차 확대해가고 있다. 이러한 유전정보는 활용범위는 다양하지만 의료정보의 특별한 한 형태로 인식되고 있다[33].

3. 의료정보의 성질

의료정보의 법적 성질을 보면 특별하게 보호되는 개인의 내밀한 영역에 속하는 '민감함 정보'라고 할 수 있다[34]. 이것은 다시 특별한 종류의 개인정보라고 말하기도 한다. 이와 같은 특별한 주의가 필요한 환자의 비밀은 이미 고대 히포크라테스 선서에 나올 정도로 의료인들이 당연히 지켜야 할 직업에 따르는 행동규약인 묵비의무로 보호되어 왔다. 이처럼 의료정보는 일반 개인정보와는 달리 민감한 정보로서 그 수집과 처리에서 매우 엄격한 제한을 받고 있으며, 이것은 의료인 및 기타 관계인에게 비밀유지의무를 부과하게 되는 것이다.

4. 의료정보의 특수성

의료정보는 일반적인 개인정보와는 다른 특수한 성격을 가지고 있다고 한다. 첫째, 의료목적이 일차적으로 환자의 치료에 있기 때문에 통상 환자 개인정보는 의료기관이 진료과정을 통해서 수집 · 축적된다는 것이다. 둘째, 의료정보에는 사회적 · 심리적으로 영향을 미칠 수 있는 중대한 내용

33) 전영주, 전게논문, 527면.
34) 길준규, 전게논문, 125면.

의 정보가 포함되어 있다는 점이다. 셋째, 부차적 목적의 중요성. 즉, 오늘날 의료정보의 유용성이 특히 강조되고 있는 것이 의학연구와 의학교육, 공중위생 등의 경우로서 “공익”이 부차적인 목적이라는 것이다[35].

가. 정보발생 및 수수의 특수성

의료정보는 환자와 의사의 진료과정에서 발생 및 수수되는 특징이 있다. 환자는 의사의 전문성을 신뢰하여 자신의 개인정보를 제공하고, 의료전문가인 의사는 진찰·검사 등을 통해서 환자의 의료정보 수집에 노력하는 한편, 설명의무라는 형식으로 환자에게 진료과정에서 취득한 의료정보를 제공하게 된다. 이와 같은 의사와 환자의 관계는 다른 개인정보의 경우 보다 정보에 관한 양자의 협동성과 신뢰성이 높게 요구되며 환자 본인의 참여도 강하게 요청된다.

나. 정보 내용의 중요성

의료정보는 다른 개인정보와 달리 사회적·심리적으로 심각한 영향을 미칠 수 있는 중요한 내용들이 포함되어 있다는 것이다. 이러한 이유로 의료에 대한 개인정보인 의료정보는 의료기관 이외에도 여러 곳에서 다양한 목적으로 사용할 가능성을 가지고 있다. 예컨대 건강보험관리공단과 심사평가원에서는 정기적으로 환자의 의료정보를 받고 있으며, 보험회사 또한 의료정보 수집을 위해 다양하게 노력하고 있다. 이러한 의료정보의 특성은 의료정보가 보호되어야 하는 중요한 시작점이 되는 것이다.

---

35) 장석천, 전게논문, 164-165면.

IV. 의료정보와 보안

1. 보호와 보안

정보를 관리하는 데 있어서 중요한 것이 보안이 될 것이다. 특히 IT 강국으로 자부하는 우리나라에서도 '보안' 문제의 심각성을 미리 인식하고 '정보보호'라는 이름으로 산업과 기술, 정책의 정체성을 정립한 바 있다.

'정보보호'는 특정 실체를 보호한다는 수동적 개념으로 이해될 수 있기 때문에 '정보보안'보다 적극성이 떨어지게 비추어 질 수 있어 최근 정부에서도 '정보보안'으로 용어를 바꾸어 사용하고 있다[36].

정보보호와 정보보안이 큰 차이가 있는 개념은 아니다. 중요한 것은 개인정보이건 의료정보이건 인터넷과 IT기술의 발전으로 인해 점차 침해의 위험성이 광범위해지고 고도화 되고 있다는 점이다.

최근 발생한 옥션과 하나로 통신, GS 칼텍스에서 개인정보의 대량 유출 사건이 말해 주듯이 이제 정보의 침해와 유출은 어느 특정 개인만의 문제가 아니라 정보화 사회 구성원 전부에 해당하는 심각한 문제로 대두되고 있는 것이다.

2. 의료정보 수집 및 이용현황

의료정보는 개인정보의 한 형태로서 1급 개인정보에 해당한다. 의료정보는 환자 진료정보와 관련된 정보 전체를 의미하는 것[37]으로서 개인의 건강상태에 관한 지극히 사적인 정보로서, 본인 이외의 사람에게 알려질 경우 해당 개인에게 매우 불리한 상황이 발생할 수 있다. 따라서 의료법 제19조에서 비밀누설금지를 규정하고 있는 것과 같이 개인에 관한 의료정

---

36) 김홍선, "보안은 기술이 아니라 마인드다", 안철수연구소 홈페이지, 김홍선CEO 칼럼.
37) 박정화, 「전자의무기록의 활용과 의료정보 보호방안에 관한 연구」, 석사학위논문, 연세대대학원, 2005, 7면.

보는 환자 본인 이외의 사람들에게 알리지 않는 것이 원칙이다[38].

개인의료정보는 특별한 사유가 없는 한 대규모로 수집하거나 이용하는 것이 법적으로 금지되어있다. 그러나 몇 가지 이유로 개인의료정보를 대량으로 보유하거나 제공하는 경우가 있는데, 우선 ① 개별 의료기관에서 진료목적으로 진료를 받은 환자들의 정보를 보유하는 경우, ② 의료기관 간 환자의 이송 등에 따라 타 의료기관에 정보를 제공하는 경우, ③ 국민건강보험법에 의하여 건강보험 청구를 위하여 국민건강보험공단에 정보를 제공하고 공단에서 이를 보유하는 경우 등이 있다. ④ 이외에도 법원이나 검찰 및 경찰에 대한 정보의 제공, 의학연구 등을 위한 정보의 이용 등이 있다[39].

가. 개별의료기관의 의료정보

(1) 환자 진료기록

개별 환자에 관한 의료정보는 진료기록부로 통칭된다. 의료법 제21조(진료기록부 등)에서 의료인의 진료기록 작성의무에 대하여 규정하고 있으며 2002년 3월 30일 의료법 개정 시에 21조의 2(전자의무기록)가 추가되어 전자의무기록에 법적인 효력을 부여하였다. 진료기록부에 기재하여야 하는 사항은 의료법시행규칙 제17조(진료기록부 등의 기재사항)에 명시되어 있고, 의료법시행규칙 제18조(진료에 관한 기록의 보존)에서 진료기록부 내용에 따라서 보존 연한을 규정하고 있다.

(2) 의료정보의 정보화

기존 의료정보의 기록형태는 종이로 된 일반 파일로 보관하고 있는 형태

---

38) 이미영·박영임, "간호사의 환자 프라이버시 보호행동에 대한 인식과 실천", 『임상간호연구』, 제11권 제1호, 2005, 7면 : 한국정보보호진흥원, 전게서, 2002, 190면.

39) 박정화, 전게논문, 26-27면.

이며 보존연한 이후에는 일부 마이크로필름이나 광디스크 등으로 보관하고 있었다. 그러나 정보기술의 발전과 전자의무기록이 법적 효력을 갖게 되면서 전자의무기록(EMR 또는 EHR)[40]으로 대체되고 있으며 처방전전달시스템(OCS)[41], 의료영상저장전송시스템(PACS)[42] 등이 도입되고 있다.

나. 의료기관 간 정보교환

의료기관간의 정보교환은 환자이송에 따른 진료기록이나 진단서에 의해 이루어진다. 교환방법은 아직까지 문서에 의한 것이 대부분을 차지하고 있으나, 최근 종합전문요양기관을 중심으로 협력관계를 형성한 의료기관간에 진료의뢰 및 회송 시 진료정보의 신속한 공유에 대한 필요성으로 인터넷상에서 환자 진료정보를 조회할 수 있는 시스템을 개발하여 운영하는 경우가 증가하고 있다.

다. 건강보험관련 정보교환

개인의료정보의 교환이나 수집이 가장 대규모로 발생하는 경우가 의료기관에서 건강보험진료비 청구를 위하여 건강보험심사평가원에 진료내역을 보낼 때이다. 각 의료기관에서는 청구를 위하여 해당 의료기관에서 진료를 받은 건강보험 환자의 진료내역을 상세히 보내야 한다. 이때에는 환자의 성명, 주민번호 등 인적사항부터 질병에 관한 정보, 검사 등 진료행위에 관

---

40) 전자의무기록 (EMR: Electronic Medical Records, EHR: Electronic Health Records)
종이매체에 의해 기록되어온 모든 의료기록을 그 업무처리 구조나 정보의 범위, 정보내용에 있어 변형 없이 동일하게 전산화를 통해 업그레이드 시킨 형태.

41) 처방전전달시스템 (OCS: Order Communication System)
각종 의학정보 및 환자들의 진찰자료를 보관한 데이터베이스와 의사가 환자를 진단한 후 처방전을 통신망을 통해 각 해당 진료부서로 전달하는 시스템으로서 환자의 등록에서 진료 수납까지 원내의 모든 데이터를 관리 전달하는 것은 물론 병원의 모든 행정을 효율적으로 관리할 수 있도록 하는 통합 의료정보 시스템.

42) 의료영상저장전송시스템 (PACS: Picture Archiving and Communication System)
디지털로 저장되어 있는 고해상도의 의료영상을 네트워크와 컴퓨터를 이용해서 조회할 수 있는 시스템.

한 정보, 투약 등 치료에 관한 정보까지 거의 모든 정보를 제공하게 된다.

현재 건강보험심사평가원에서 정보를 보존해야 하는 기간은 법적으로 명시되어 있지 않으나, 요양기관의 이의제기 등에 대비하여 거의 영구 보존하고 있다. 정보 제공방법은 초기에는 서면으로 하였으나 최근에는 EDI[43]를 이용한 청구가 크게 늘어나고 있다.

라. 기타 정보이용 현황

이외에 민사 및 형사상의 이유로 법원이나 검찰 및 경찰에 정보를 제공하여 이용하는 경우가 있으나 개인의 의료정보를 많이 이용하는 경우가 의학 연구 분야이다. 의학연구는 실험실에서 하는 연구도 있으나, 대부분 그 효과 입증을 위하여 환자들을 대상으로 하는 임상 시험 단계를 거쳐야 하는 특성으로 인하여 환자들 개개인에 대한 정보가 수집·이용되고 있다.

3. 의료정보화 단계에 따른 보안위험

의료정보화는 "병원정보화 ⇒ e-Health ⇒ u-Health"로 진화하고 있다. 이에 따라 의료서비스가 질병치료는 물론 건강한 상태의 지속적 관리와 질병예방까지 개념이 확장되고 있다. 이러한 의료정보화의 발전 단계에 따라 보안위험은 점증되고 있다[44].

가. 병원 정보화 단계

수기로 작성되던 의료정보가 전산화되면서 네트워크 기반의 중앙 집중 시스템에 저장되어 관리 및 처리되고 있다. 소규모로 분산되어 저장·처리되던 의료정보가 대규모 데이터베이스로 집적 및 통합되면서 보안위협은

---

43) Electronic Data Interchange 기업 간 데이터 교환을 위해 지정한 데이터, 문서 등의 표준화시스템.

44) 상세한 내용은, 김홍근·김윤정, 전게논문, 6-8면 참조.

더욱 커졌다. 또한 디지털 병원으로 발전함에 따라 각종 의료정보가 디지털로 처리되면서 각종 의료기기들에 의한 의료정보의 생성이 폭발적으로 증가하고 있다.

의료정보에 대한 권한이 없는 자의 접근으로 개인의 의료정보가 노출되거나 조작될 수 있다. 특히 진료와 상관없는 직원의 전자의무기록 열람 가능성이나, 진료기록 관리 전산담당직원의 유출 가능성 등 내부자의 고의·과실로 인한 개인 의료정보 유출은 병원정보화의 가장 큰 위협이 되고 있다. 개인 의료정보의 보호를 위해 인증·암호화를 통해 보안을 강화한 의료정보시스템의 구축이 필요하고 의료인 및 의료관계인의 직업윤리 강화 등의 방안이 필요할 것이다.

나. e-Health 단계

원격의료로 대표되는 e-Health의 경우, 의료정보의 이동성이 증가하고 이동량도 많아지면서 의료정보에 대한 외부로부터의 공격가능성이 증가하고 있다. 인터넷을 활용한 건강정보 제공 사이트에 가입하여 건강정보를 주고받는 의료서비스의 경우, 축척된 개인의 의료정보가 외부의 공격자에게 공격당해 개인의 민감한 의료정보가 유출될 수 있다. 또한 원격지 환자를 진료하는 원격의료에서 교환 및 저장되는 데이터에 대한 보안장치가 허술한 경우, 해커 등 공격자들로부터 쉽게 공격받아 개인의 의료정보가 유출될 수 있다. 현행 의료법 제34조(원격의료)[45] 및 의료법시행규칙 제29조(원격의료의 시설 및 장비)에서 원격의료를 위한 시스템에 대한 제도적 규정과 원격의료인과 현지의료인의 책임의 범위에 대해서 규정하고 있어 시대적 상황을 반영하고 있으며, 과거에 비해 진일보하기는 하였지만 보안위협에 대한 근본적인 해결이 이루어진 것은 아니다.

---

45) 2007.4.11. 의료법 개정 시 처음 도입되었다.

다. u-Health 단계

센싱과 모니터링 기능으로 대표되는 u-Health의 경우, 센싱기능의 부정확성으로 인한 진단 오류, RFID[46] 등을 이용한 과도한 개인정보 수집으로 인한 프라이버시침해 등의 가능성이 증가된다. u-Health 서비스의 하나인 스마트의료 홈시스템에서 홈패드와 연결된 측정기기로 혈압, 체지방을 체크하여 병원시스템과 연결된 건강관리를 받을 경우, 센서의 인식률에 따라 데이터의 품질편차가 매우 커 진단오류가 발생할 가능성이 상존한다. 또한 건강상태를 다양하게 측정하고 진단하기 위해 복잡하고 다양하게 수집되는 개인 의료정보의 양이 폭발적으로 증가함에 따라 보안대상 또한 폭발적으로 증가한다. 이처럼 도처에 존재하는 센서를 통해 특정 개인은 물론 타인의 정보까지 과도하게 수집될 수 있으며 기타 개인정보와 결합할 경우 병원이 빅브라더로 존재할 가능성도 배제할 수 없다.

4. 의료정보 보안위협의 특성

정보보안 시스템이 일반적으로 갖추어야 할 요소로 비밀성, 무결성, 가용성이 언급된다. 각각의 요소에 대한 보안상 위협에 대해서 정리하면 다음과 같다[47].

가. 의료정보에 대한 비밀성의 위협

편재형 컴퓨팅(Pervasive Computing)[48] 기술이 실현되는 의료 환경에

---

46) RFID (radio frequency identification) 각종 물품에 소형 칩을 부착해 사물의 정보와 주변 환경정보를 무선주파수로 전송·처리하는 비접촉식 인식시스템이다. 1980년대부터 등장한 이 시스템은 DSRC (dedicated short range communication: 전용 근거리 통신) 또는 무선식별시스템이라고도 한다. 판독·해독기능이 있는 판독기와 고유 정보를 내장한 RF 태그 (RF ID tag), 운용 소프트웨어, 네트워크 등으로 구성된 전파식별시스템은 사물에 부착된 얇은 평면 형태의 태그를 식별함으로써 정보를 처리한다.

47) 상세한 내용은, 김홍근·김윤정, 전게논문, 8-9면 참조.

48) Pervasive Computing: 고도의 전자적, 특히 무선 기술과 인터넷의 융합으로 컴퓨팅

서는 환자의 의료기록에 언제 어디서나 접근 가능하며, 많은 경우 의료정보가 무선으로 전송됨에 따라 의료정보의 비밀성과 무결성의 위협이 증가하고 있다. 분절화 되어 개별적으로 접근했던 의료정보가 통합되어 관련자들이 모두 데이터베이스에 접근할 수 있고, 이에 따라 복잡하고 다양한 접근통제 규칙이 필요하게 되었다. 분산되어 있던 의료정보가 통합되면서 결과적으로 분절화 되어있던 의료정보의 비밀성 보호 수단이 없어지게 되며, 이는 정보보안에 매우 취약한 상황이 된다. 에이즈 감염, 낙태수술, 정신과 치료 등에 대한 병력이 공개될 경우 프라이버시 침해로 인한 치명적인 피해가 가능하여 데이터 중요도나 중점관리대상으로 관리되어야 하나 제도적 뒷받침이 부족한 실정이며, 접근통제 규칙을 합리적으로 설계·구현하기 위한 시스템 마련이 시급한 상황이다.

나. 의료정보에 대한 무결성의 위협

컴퓨터 바이러스 등의 악성 코드로 인한 의료정보의 파괴나 시스템 소프트웨어 버그나 하드웨어 고장으로 인한 의료정보의 변질은 잘못된 진단으로 이어져 생명에 대한 직접적인 위협의 요인이 될 가능성이 있다. 병원 내부직원에 의한 의료정보의 변질이나, 환자가 자신의 민감한 의료정보의 노출을 우려하여 잘못된 정보를 제공하여 입력되는 경우 데이터 무결성의 심각한 위협이 되기도 한다. 임상실험을 위해 필요한 의료정보로서 개인 의료정보가 경제적 가치를 갖게 될 경우, 또는 불순한 의도가 개입되는 경우 의료정보의 수정 변질이 우려된다.

장비의 접속이 점차 늘어나는 경향. 이 컴퓨팅 장비는 자동차, 도구, 가전기기, 의류, 각종 소비제품 등 거의 모든 물체에 이동식 또는 끼워 넣기 식으로 된, 네트워크를 통해 통신하고 눈에 보이지 않는 매우 작은 장비이다. 일상화된 컴퓨팅으로 사람들은 자신이 컴퓨터를 사용하고 있는지 인식하지 못하게 되고, 주변에 있는 스마트 장비들이 자신의 위치 정보와 자신이 처해 있는 상황 및 사용자에 대한 관련 데이터를 유지시켜 준다.

다. 의료정보에 대한 가용성의 위협

의료정보가 저장된 무선 단말기, 랩탑 컴퓨터 등에 대한 도난사건 발생시에 저장된 의료정보의 비밀성뿐만 아니라 가용성도 침해된다. 정전이나 홍수화재 등의 재난 발생시, 의료정보 저장매체의 물리적 손상으로 인한 가용성 침해의 위험이 있으며, 무시할 수 없는 정도의 기기 고장으로 인해 필요할 때 서비스를 제공하지 못할 수도 있다.

V. 의료정보의 침해

1. 의료정보의 유출

최근까지 의료기록은 매우 한정된 목적에 사용되었다. 개인이 의료문제에 직면했을 때 상세한 기록을 제공함으로써 상태를 더 호전시킬 수 있도록 돕는 것이었다. 그러나 오늘날 의료기록은 그 역할이 확장되어 본래 목적인 치료와 관련이 없는 영역에서도 사용된다. 예컨대, 고용주나 보험회사가 고용여부나 보험자격 여부를 결정할 때, 병원이나 종교단체에서 기부금을 부탁하는 경우에도 사용된다. 또한 마케터가 시장에서 판매선점을 위해 의료기록을 입수하려고도 한다. 과거에는 사람들이 자신의 의료기록이 최신성을 유지하고 정확하길 원했다면 요즈음 사람들은 의료기록이 불가피하게 공개될 경우 그 피해를 최소화할 수 있도록 의료기록을 따로 분류해서 보관해주길 원하고 있다[49].

앞서 살펴본 바와 같이 의료정보가 전산화 하면서 의료정보가 유출될 가능성은 점차 증가하고 있으며 이로 인한 개인의 프라이버시 침해 위험도 동시에 가중되고 있다고 볼 수 있다. 즉, 개인의료정보의 수집 및 이용

49) 진태영, 「의학적 검사 및 의무기록과 관련된 사생활의 비밀보호」, 석사학위논문, 연세대보건대학원, 2003, 49면.

현황에서 검토한 것처럼 타 의료기관, 의료보험관리기관, 공공의료기관, 정부기관 등의 기관에 제공하는 경우는 물론, 각종 보험회사, 신용조사기관, 언론기관, 사회복지프로그램기관, 제약회사, 연구기관 등에도 유출 될 수 있다.

2. 의료정보의 유출로 인한 침해

의료정보는 환자의 치료뿐만 아니라 직장생활, 유명인의 경우 그의 사회생활 전체에 미치는 영향이 치명적이다. 환자의 치료 목적으로 인지하게 된 신체적 특징, 과거 질병과 치료 경과, 성생활, 심지어는 가족들의 질병기록까지 수집, 활용되고 있기 때문에 의료기록은 개인의 불완전함을 들추어내고자 하는 사람들에게는 가장 좋은 대상이 되고 있다. 우리의 경우 건강보험과 국민연금을 둘러싼 개인의 의료정보가 주민등록번호를 매개로 한 전산화를 통해 활용되고 있기 때문에 법적 보호의 필요성이 크다고 할 수 있다[50]. 의료정보의 유출은 개인의 사회생활에도 치명타가 될 수 있으며, 특히 B형 간염이나 에이즈와 같은 경우는 한 인간의 거의 모든 생활영역[51]에 지장을 초래하고 있다[52].

3. 의료정보 침해의 유형

외부에 노출되거나 전파되어 개인의 사생활을 침해하게 되는 의료정보들의 종류와 형태는 일률적으로 객관화시키기가 어렵다. 그렇지만 의료정보의 유출로 사생활이 침해되는 유형을 정보유통의 과정에 따라보면, 환

---

50) 공종렬, 「지식정보사회의 개인정보 침해사례분석과 보호정책에 관한 연구」, 박사학위논문, 경희대대학원, 2001, 111~112면.

51) 에이즈에 대한 감염사실의 유출은 사회적인 낙인은 물론 교육 및 노동기회를 상실하게 되기도 한다. 다른 질병의 경우에도 취업문제, 보험계약 등 다양한 측면에서 피해를 당할 수 있다.

52) 진태영, 전게논문, 51면.

자로부터 정보가 수집되는 과정, 이것이 축적, 처리되는 과정, 의료정보가 이용되는 과정, 유통되는 과정으로 구분해 볼 수 있다[53].

가. 의료정보의 불법 모집

불법 수단이나 방법에 의하여 의료정보를 수집하는 경우와 수집이 금지되는 의료정보를 수집한 경우이다. 의료정보 수집의 불법적인 수단이나 방법이 환자 자신이 의료정보 유통을 조종할 수 있는 권리를 침해하는 것으로 인정되는 경우로서, 컴퓨터의 데이터베이스에 불법 접근하여 수집하는 경우를 생각해 볼 수 있다.

나. 의료정보의 불법 축적, 처리

수집된 의료정보를 임의로 고치거나 변경, 삭제, 추가 등을 하여 환자에 대한 부정확한 정보로 생성 및 변경되어 이를 기초로 한 환자 치료행위의 장애와 사회적, 문화적, 인간적 관계의 치명적 결과를 야기할 위험성이다.

다. 의료정보의 불법 이용

의료정보를 권한 없이 불법으로 이용하는 것이 침해에 해당하는 것은 물론이며, 의료정보가 치료행위 이외의 목적으로 사용되는 경우도 불법 이용에 해당할 것이다.

라. 의료정보의 불법 유통

개인 의료정보가 본인의 의사에 반하여 불법으로 유통되어서는 안 된다. 다만 헌법상의 알 권리 또는 정보유통, 정보공개의 권리와 모순되는 경우도 발생할 수 있을 것인 바 이 때는 상호 균형의 문제가 발생할 것이다.

---

53) 김동규 외, 『의료부문의 정보이용 활성화』, 한국보건사회연구원, 1995, 91-92면.

4. 의료정보 침해와 피해구제 사례

의료정보의 유출이 개인의 사생활이 침해로 되는 것은 환자의 자기결정권에 대한 침해로 설명하는 하는 것이 일반적이다. 즉 환자는 자신의 질병에 대하여 치료를 받을 것인지, 치료를 받는다면 어떤 방법으로 어느 정도로 받을 것인지 여부에 대하여 스스로 결정할 권리를 가지며 이를 환자의 자기결정권이라고 한다[54]. 자기결정권의 개념은 헌법 10조에 근거를 두고 있다.

개인정보가 침해 된 경우 개인정보 분쟁조정위원회에 피해구제 신청을 하여 조정결정을 받을 수가 있는데 위원회에 접수되어 처리된 사례 몇 가지를 살펴보기로 하자.

[사례 1] 이용자의 개인정보를 동의 없이 제3자에게 제공한 건[55]

〖병원이 의무기록상의 개인정보를 건강보조식품회사에 동의 없이 제공〗

환자 A는 X 병원에서 건강검진을 받은 사실이 있는데 이후 Y 건강식품회사로부터 건강보조식품 관련 임상실험에 참여해 줄 것을 우편으로 요청받자, X 병원이 환자 A의 개인정보를 Y 회사에 동의 없이 제공하였다고 주장하며 이로 인한 정신적 피해를 보상할 것을 요구 한 건

[사례 2] 사업자가 개인정보보호 기술적 · 관리적 조치를 미비한 사례

〖성형외과 병원 회원정보가 웹사이트를 통해 노출된 건〗

환자 A는 ○○ 검색사이트에서 자신의 성명을 검색하면 과거 자신이 회원으로 가입한 바 있는 X 성형외과 병원의 회원정보 리스트가 그대로 노출되는 것을 발견하고, X 성형외과 병원의 개인정보 보호 미 조치로 인해 알리고 싶지 않은 개인적인 사실이 노출되어 정신적 피해를 입었다고 주장하며 손해배상을 요구 한 건

---

54) 전영주, 전게논문, 527면.
55) 강달천, 전게서, 114면 이하 참조.

[사례 3] 기타 사례[56]

〖성형외과병원이 고객의 성형수술장면 동영상을 병원 웹사이트에 무단으로 게재한 건〗

환자 A는 X 성형외과에서 성형수술을 받았는바, 이후 자신의 성형수술 장면 동영상이 X 성형외과 웹사이트에 무단으로 게재되어있다고 주장하면서 이로 인해 입은 정신적 피해를 배상할 것을 요구 한 건. (성형외과에서 수술 받은 후와 수술 전을 비교한 사진을 무단으로 게재한 사건도 있음.)

VI. 의료정보의 보호

1. 의료정보의 보호

"의료정보의 보호"는 진료를 받는 환자에 대해서 의료인이나 의료기관이 취득하고 보유하는 개인정보가 적절히 이용 및 관리되도록 함으로서 환자 개인의 프라이버시 보호와 그 이외의 정당한 권리 · 이익을 보호하는 것이라고 할 수 있다. 의료정보의 보호를 다음과 같이 누가 어떤 목적으로 어떻게 이용하는가에 따라 나누어 생각해 볼 수 있을 것이다[57].

가. 사용자

의료정보를 누가 사용하는가에 대해서는 개인에게 의료를 시술하는 의료기관 내부에서 사용하는 것인지, 아니면 외부에서 사용하는 것인지에 따라 나누어질 수 있다. 의료기관 내부의 경우에도 환자를 직접 치료하는 담당 의사인지, 아니면 다른 의사인지, 그리고 간호사, 약사, 검사자, 사무담당

56) 개인정보분쟁조정위원회, 『2004 개인정보분쟁조정사례집』, 한국정보보호진흥원, 2004. 292면.

57) 장석천, 전게논문, 163면.

자, 경영자, 기타 병원 근무자 등 중에서 누가 사용하는지가 문제로 된다. 의료기관 외부의 경우 다른 의료기관과 연구기관, 국가와 지방공공단체의 의료행정 담당기관, 건강보험공단, 보험회사, 제약회사 등 여러 기관과 개인이 이용하는 경우를 생각해 볼 수 있을 것이다. 그리고 경찰과 검찰 · 법원 · 변호사 등 사법기관 등이 이용하는 경우도 고려해 볼 수 있다.

나. 사용 목적

의료정보를 어떤 목적으로 사용하는가 하는 문제이다. 이는 환자의 치료를 위해서 직접적으로 필요한 이용, 즉 치료목적과 그 이외의 목적에 이용하는 경우로 크게 나누어 볼 수 있다. 의학의 연구와 교육, 약과 의료기구의 개발, 상품과 서비스의 마케팅 등은 치료목적 이외의 이용에 해당한다.

다. 사용 방법

의료정보를 어떻게 사용하는가이다. 의료정보를 서류 형태로 사용하는 것인지 아니면 전산화해서 사용하는 것인지, 그리고 개인정보를 어느 정도 익명화해서 사용하는 것인지 등이 문제로 된다.

2. 현행 의료정보 보호관련 법률

아직까지 우리나라에는 의료정보보호를 위한 체계적인 제도는 마련되어 있지 않고 있으며, 개별 법률에서 부분적으로 의료정보의 보호를 도모하고 있다. 의료정보 보호에 대하여 규정하고 있는 보건의료 관련 법률로는 의료법, 응급의료에 관한 법률, 전염병예방법, 후천성면역결핍증 예방법, 국민건강보험법, 의료기사 등에 관한 법률이 있다.

가. 보건의료 관련법

현행 '의료법'은 제18조(진단서 등), 제19조(비밀누설의 금지)[58], 제20

조(기록 열람 등), 제21조(진료기록부 등), 제21조의2(전자의무기록)가 있으며, '응급의료에 관한 법률'은 제40조(비밀 준수의 의무)가 있고, '의료기사 등에 관한 법률'은 제10조(비밀누설의 금지)가 있다. '전염병예방법'은 제4조(의사 등의 신고), 제7조(전염병환자등의 명부작성), 제54조의6(비밀누설금지)이 있고, '후천성면역결핍증예방법'은 제5조(의사 또는 의료기관등의 신고), 제6조(감염자 명부의 작성·보고), 제7조(비밀누설금지)가 있다. '국민건강보험법'은 제82조(신고 등,) 제86조(비밀의 유지)가 있다. '생명윤리 및 안전에 관한 법률'은 제48조(비밀누설 등의 금지), 제34조(유전자은행의 장의 준수사항)을 규정하고 있다.

나. 기타법률

보건의료 관계법 이외의 법률에서도 의료정보 보호를 위한 규정을 두고 있다. 대표적인 것이 '형법'제317조의 업무상 취득한 비밀의 누설금지 규정을 들 수 있고, '전자서명법'은 제24조(개인정보의 보호)에서 관련규정을 찾을 수 있으며, '공공기관의 개인정보보호에 관한 법률'은 제9조(개인정보의 안전성 확보 등), 제10조(처리정보의 이용 및 제공의 제한), 제11조(개인정보취급자의 의무), 제22조(공공기관외의 개인 또는 단체의 개인정보보호)규정이 있고, '정보통신망이용촉진및정보보호등에관한법률'제49조(비밀 등의 보호)에서 관련내용을 규정하고 있다.

3. 의료정보 보호를 위한 제도

보건복지부는 2006년 보건의료정보화 사업추진과 관련하여 국민의 건강정보보호를 위한 주요사항들을 논의하기 위한 "건강정보보호자문위원

---

58) 오상원, "의사의 직업비밀 유지보호와 정보보호", 『법학연구』, 4권, 홍익대학교 법학연구소, 2002. 의사의 비밀유지의무에 대해서 상세 내용 참조할 만하다. 특히 공공기관의 개인정보보호에 관한 법률과의 관계에 대해서도 도움이 된다.

회"를 운영 중에 있다. 또한 개인의 의료정보 등 중요정보를 다루고 있는 건강보험심사평가원은 국보연[59] 산하 정보보안협의회에 가입하여 정보보안업무관련 정보교류, 정책제안 등을 수행하고 있다[60].

4. 해외 입법례

가. 미국

미국은 "건강보험의 이전과 책임에 관한 법률"(HIPAA: Health Insurance Portability and Accountability Act, 1996)[61]이 제정되기 전까지 개인의료정보의 보호에 대해 정부기관이나 민간부분에 모두 적용되는 법률이 없었다. HIPAA는 5편으로 구성되어 있는데 제2편 F부 "행정의 간소화"부분이 개인의료정보의 보호에 관한 법률 제정에 근간이 되었다. 이에 따라서 개인의료정보 보호를 위해 "식별가능한 개인보건의료정보의 보호에 관한 표준"(Standaeds for Privacy of Individually Identifiable Health Information) 규칙이 제정되었다[62]. HIPAA와 동 규칙을 통해 의료정보서비스가 가능하도록 법제화하고, 전자의무기록 표준화 등 정부차원의 의료정보화를 적극 추진 중에 있으며, 전자의료정보의 기술, 관리, 물리적 대책에 대한 규정을 두고 있으며 원격의료정보에 대해서도 준용하고 있다.

나. EU

EU는 'e-Europe 2005'에 기반하여 광대역 네트워크 구축을 통한 의료

---

59) 국가보안연구소(NSRI: National Security Research Institute).

60) 김홍근·김윤정, 전게논문, 14면.

61) HIPAA는 미국 보건성에서 발표한 연방정책의 지침서 및 국가 표준 법안이다. 상세한 내용은, 김민호, "의료정보의 현황과 입법과제", 『정보시스템의 구축 운영과 입법과제』, 한국법제연구원, 2005, 49면 이하 : 백윤철, "헌법상 환자의 의료정보에 대한 권리에 관한 연구: 미국의 HIPAA프라이버시규칙을 중심으로", 『헌법학연구』, 제11호 제3호, 한국헌법학회, 2005, 395면 이하.

62) 장석천, 전게논문, 16면 이하 : 길준규, 전게논문, 127면.

정보화를 계획 중에 있다. EU는 의료기기의 안전조건을 충족시키기 위해 CE(Communaute Europeene)마크[63] 부착을 의무화하고 기술표준, 제도 연구 등을 활발히 수행 중에 있다. EU의 정보사회기술(IST)의 e-Health 활성화 정책과 함께 건강관련 웹사이트의 기준을 제공하고 이를 EU 회원국들이 준수할 것을 권고하고 있으며 웹사이트의 프라이버시 정책, 개인 의료정보보호를 위한 보안정책 등을 제공하고 있다[64].

의료정보에 대해 "유럽인권협약"(European Convention of Human Rights)에 근거하여 EU는 "유럽공동체정보보호지침"(european Community Directive on Data Protection)을 제정하여 의료정보의 수집 · 저장 · 이용 · 전달에 관하여 당사자의 명문상의 동의가 있거나, 응급상황인 경우를 제외하고는 정보의 공개 등을 원칙적으로 금하고 있다[65].

다. 독일

독일은 2001년 EU의 "유럽공동체정보보호지침"을 받아들여 "연방정보보호법"을 제정하였다. 이 규정을 통해서 의료정보의 생산자는 치료위탁을 통하여 환자의 이익과 의료인의 의무 간에 합리적인 조정이 가능하게 되었다[66].

라. 일본

일본은 1974년부터 후생성과 통상산업성이 공동 출자하여 의료정보시스템 개발센터(MEDIS-DC)를 설립하여 보건의료정보시스템에 대한 종합적인 조사, 연구사업을 실시하고 있다.

---

63) CE 마크: 인체의 안전, 건강, 환경 및 보호 등과 관련된 13개 제품 품목별로 각종제품에 대해 부착하는 마크로 의료장비 분야에 시행 중이다.
64) 김홍근·김윤정, 전게논문, 14~16면.
65) 장석천, 전게논문, 169면 이하.
66) 상세한 내용은, 장석천, 전게논문, 169면 이하 : 길준규, 전게논문, 127면.

일본의 개인정보보호에 관한 법률들은 1980년 OECD의 “프라이버시 보호와 개인 데이터의 국제유통에 대한 가이드라인에 관한 이사회 권고”에서 제시한 OECD 개인정보보호 8원칙에 영향을 받았다[67]. 2003년 5월 개인정보보호법을 통해 환자의 의무기록을 진료 목적이라도 다른 의료진에 통보할 경우 환자의 동의를 거치도록 의무화하고 있다. 일본의 의료정보보호에 대한 법령은 공공부문과 민간부문을 별개로 규율하고 있다. 공공부문은 ‘행정기관이 보유하는 개인정보의 보호에 관한 법률’과 ‘독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률’ 및 ‘지방자치단체의 조례’ 등에 의해서 규율되고, 민간부문은 ‘개인정보의 보호에 관한 법률’에 의해서 규율된다. 그리고 이러한 법률들을 뒷받침하는 각종 가이드라인이 관련 부서에 의해 제정되어 있다[68].

또한 일본은 1994년 4월, 전자의무기록의 적법성을 인정하고 고의 또는 과실에 의한 허위 입력, 수정 입력 등을 방지하였으며, 책임소재를 명확히 하는 내용의 법안을 채택한 바 있다.

5. 의료정보 보호방안

가. 의료정보 처리단계 측면

(1) 의료정보 수집단계

정보 수집단계에서 최우선으로 고려할 사항은 해당 정보가 민감한 정보인지 아닌지 평가해야한다. ‘공공정보법’ 제4조제1항은 “사상 · 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보”를 수집하면 안 된다고 하고 있으며, ‘통신정보법’ 제23조 제1항도 “사상 · 신조 · 과거의 병력 등 개인의 권리 · 이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보”의 수집을 금지하고 있다. 즉 의료정보는 민감한 정보로서 원칙

67) 상세한 내용은, 백윤철 외, 전게서, 235면 이하 참조.
68) 장석천, 전게논문, 170면.

적으로 수집이 금지되어 있는 개인정보인 것이다.

의료정보의 수집이 예외적으로 허용되는 경우는 정보주체의 동의가 있거나 다른 법률에 의해서 수집대상으로 명시된 경우가 될 것이다.

(2) 의료정보 축적 및 처리단계

의료정보가 처리되고 축적, 저장되는 단계는 구체적으로 의료인의 진료행위에 따른 의무기록의 작성 및 보관으로 이루어지게 된다. 의료정보화 단계가 앞서 살펴본 바와 같이 e-Health를 거쳐 u-Health의 단계로 발전 할수록 문제가 발생할 것이다. 이러한 환경에서 정보의 안전을 확보하기 위해서는 권한이 있는 자만이 각종 인증과정을 통해서 전자의무기록을 작성 할 수 있도록 하고, 기존에 저장된 의료정보시스템의 접근도 그 범위를 필요 최소한으로 해야 할 것이다. 특히 환자 정보에 대해서도 익명화 등 암호화 처리는 필수라 할 것이다. 즉 직접 진료하는 사람은 물론 다른 의료관계인 이라고 해도 환자 정보 중에서 굳이 몰라도 되는 사항들(주민번호, 주소 등)에 대해서는 알 수 없도록 처리해야 할 것이다.

(3) 의료정보 이용 및 유통단계

의료정보의 경우 정보에 대한 접근과 이용 및 전달의 문제가 발생한다. 즉, 타 의료기관으로 공개 또는 전달하거나 건강보험공단, 심평원 등으로 보내고, 검찰 등 국가기관의 요청에 따라서 의료정보를 공개하는 일이 발생한다. 현실적으로 환자정보보호의 문제에서 가장 문제가 되는 사항이라고 할 것이다. 의료법에서 규정하고 있는 경우 즉, 타 법률에 관련 규정이 있거나 의료법에서 정하고 있는 인척관계 또는 위임장을 갖고 있는 대리인 이외에는 의료정보의 공개 및 전달을 엄격히 제한해야 할 것이다. 특히 보험회사에서 환자의 의료정보에 대해 위임장을 받아서 여러 번 복사해서 사용하는 등 불법적인 일이 발생하고, 이에 따라서 병원이 환자와의 소송[69]에 휘

말리게 되는 경우도 발생하고 있으므로 각별히 유의해야 할 사항이다.

나. 기술·관리적 측면

의료정보 처리 시스템의 안전신뢰성이 강화 되어야 한다. 컴퓨팅 시스템에서 안전신뢰성이란 서비스를 신뢰할만한 수준으로 제공할 수 있는 능력으로 정의 되는데, 보안의 속성인 비밀성, 무결성, 가용성을 포함하며, 정확한 서비스의 연속과 환자에게 치명적인 결과를 야기하지 않는 것을 포괄하는 개념이다[70]. 의료정보는 의료인과 의료진단용 장비에 의해 생성되며, 이들 정보의 기밀성, 무결성, 가용성 등을 의료정보의 라이프 사이클동안 보장하기 위한 관리가 지속되어야 한다. 의료정보 처리 시스템은 외부 공격이나 결함으로부터 벗어나 정확한 서비스를 제공해야 된다. 이러한 측면에서 다음과 같은 것들을 고려해 볼 수 있다.

(1) 의료정보의 분산 저장

환자의 의료정보를 다루는 시스템의 저장 용량을 제한한다. 예를 들어 최대 10만 명까지 환자 레코드를 제한하여 저장 하도록 한다. 이는 분산을 통하여 외부 침해가 발생하더라도 피해가 한정적으로 이루어지도록 하기 위함이다.

(2) 의료정보의 암호 처리

저장 및 전송 과정에서는 반드시 암호처리를 의무적으로 사용하여 사용자를 가장한 공격, 통신 도청 등에 대해서도 의료정보를 보호할 수 있도록 한다.

---

69) 법원의 문서송부 촉탁에 대해서 환자 진료기록을 환자 동의 없이 법원에 보냈다는 이유로 환자가 병원을 고소하였고, 검찰이 벌금형을 부과하였고 이에 대해 병원은 정식소송을 제기하였다. 1심법원은 병원이 의료법을 위반하였다는 취지로 벌금형을 부과하였다(2006.12.14. 선고 2006고정403 판결). 그러나 2심법원은 무죄를 선고하였고(2007.5.10. 선고 2006노3797 판결), 대법원에서 무죄로 원심 확정되었다(2007.7.27. 선고 2007도4313 판결).

70) 김홍근·김윤정, 전게논문, 18면.

(3) 의료 종사자들에 대한 교육 강화

의료정보를 주로 취급하는 의료 종사자들에 대한 보안 교육 및 훈련을 강화한다. 환자 프라이버시 보호에 관한 윤리 또는 의무를 의료종사자들에게 부과한다.

(4) 합리적인 의료정보 접근 통제 규칙 수립

의료정보에 대한 최대의 보안위협인 내부자의 오용 및 남용을 방지하기 위한 접근 통제를 적극적으로 실행하기 위하여, 최소한의 관련자만이 접근할 수 있도록 접근통제 원칙을 제정한다. 개인의 프라이버시 정보를 보험, 행정, 사법 등에서 접근하는 데 있어 정치적 압력을 최대한 차단하기 위한 사회적 합의 도출이 필요하다.

(5) 진료정보의 장기 보관을 위한 기술 개발

법적 보관 기간을 경과한 의료정보는 추후 있을지도 모를 법적 분쟁에 대비하여 계속하여 보관할 필요가 있다. 따라서 분산되어 있는 의료정보를 백업 보관하기 위한 자동화된 보관 기술, 시스템 및 관리체계를 개발할 필요성이 있다.

다. 법 제도적 측면

의료법 개인정보보호 조항에는 원격의료 과정에서 취득한 환자의 개인정보 등에 대해 별도의 보호규정을 두고 있지 않으며 비밀누출의 경우, 정보통신망이용촉진및정보보호등에관한법률(이하 정보통신망법)의 관련조항보다 약한 처벌규정으로 형평성의 문제가 제기되고 있다. 즉, 정보통신망법의 경우 정보유출금지[71]를 어겼을 때 5년 이하 징역과 5천만원 이하 벌금형을 규정[72]하고 있으나 의료법은 3년 이하 징역과 1천만원 이하로

71) 정보통신망이용촉진및정보보호등에관한법률 제49조(비밀 등의 보호).

규정[73]하고 있다. 개인의 의료정보보호의 문제는 매우 중요하므로 정보통신망법에서의 기준으로 강화하는 것이 필요하다.

의료법의 비밀누설 금지조항은 친고죄[74]로 설정되어 개인정보보호의 사각지대가 발생할 가능성이 있다. 정보통신망법은 친고죄가 아니며 개인정보침해의 경우 당사자의 합의가 있더라도 강력히 처벌하도록 규정하고 있다. 의료정보의 중요성으로 보아 엄격한 처벌원칙이 필요하다.

의료법은 원격의료의 시설과 장비 구비를 규정하고 있으나 보안과 관련된 상세한 필수조항 구비 등은 마련되어 있지 않다. 의료법 시행규칙 제29조(원격의료의 시설 및 장비)에서 원격의료에 기본적으로 필요한 데이터 및 화상을 전송 · 수신할 수 있는 단말기, 서버, 정보통신망 등의 장비를 갖추어야 함을 규정하고 있으나 장치의 기준이나 보안 필수조항 등은 규정하지 않고 있다. 원격의료나 전자의무기록 등을 저장하는 장비의 보호를 위한 인적 요건과 물리적 요건 구비조항이 마련되어야 하며 미국 HIPAA등을 참조한 세부요건의 마련도 필요하다. 또한 의료법에는 의료시스템의 관리점검이나 보고 등의 규정조항이 없어 시스템운영에 필요한 최소한의 관리내용이 없어 이를 보완하는 조치가 필요하다.

개인정보 보호를 위한 별도의 입법논의가 비교적 활발하게 이루어지고 있다. 앞서 살펴본 바와 같이 각각의 개별법에서 필요한 경우에 개인정보 보호를 위한 규정이 있을 뿐 종합적이고 통합적인 개인정보 보호를 위한 일반법은 없는 상황이다. 의료정보 보호를 위한 개별법 또한 없는 상황인데 의료법 개정을 통해서 규정하면 된다고 볼 수도 있지만, 개인정보 및 의료정보 보호를 종합적으로 하기에는 미흡하고 항상 한계에 노출 될 수밖에 없으므로 별도의 의료정보관련 개인정보보보호법의 입법이 필요하게 된다[75].

---

72) 정보통신망이용촉진및정보보호등에관한법률 제62조(벌칙).
73) 의료법 제67조(벌칙).
74) 의료법 제67조(벌칙).
75) 전영주, 전게논문, 536면 : 전영주, "의료법상 의료정보 보호방안 -의무기록 보호를 중심으로", 『법학연구』, 제28집, 2007, 480면 : 장석천, 전게논문, 177면 이하 : 백윤철

VII. 맺음말

의료정보는 민감한 개인정보 중 하나로서 개인의 고유하고 다양한 정보들이 포함되어 있다. 의료정보는 개인의 건강상태와 병력까지 알 수 있어, 본인 이외의 제3자에게 유출될 경우 심각한 문제를 발생시킬 가능성이 있다. 그만큼 제3자가 많은 관심을 갖는 정보이다. 여러 가지 경로를 통하여 수집되는 의료정보는 수집기관이 본래의 정보수집 목적 이외의 용도로 사용하게 되는 경우 개인의 의도와는 전혀 다른 결과를 초래하기도 한다. 따라서 정보에 대한 기밀유지가 필요하다.

또한 의료정보를 근거로 한 차별 금지가 요구된다. 의료정보가 외부로 유출 될 경우 사회적으로 낙인이 찍히거나 고용, 보험, 학교 등에서 차별을 받을 가능성이 높기 때문이다.

현재 의료 체계상 환자의 의료정보에 대한 보호 및 보안은 의료기관이 책임지고 있다. 그러나 의료정보화 발전에 따라 의료정보에 대한 관심이 고조되고 있어 이를 합리적으로 관리할 법 제도적 및 기술·관리적 측면에서 보완할 점이 많다. 의료정보를 직접 생산 및 관리하는 해당 의료 기관만이 아니라 의료정보의 수집 및 이용과정에서 관여하는 모든 기관들이 책임을 부담할 수 있도록 하여야 한다.

최근 금융위원회가 보험사기 등을 조사하기 위해 국민건강보험공단에 저장되어 있는 개인의 질병·치료정보를 열람하겠다고 하여 논란이 된 일은 시사 하는바가 크다. 금융위원회는 검찰과 같은 수사기관이 아니면서 개인의 세세한 정보를 보겠다는 것인데, 잘못하면 민간보험사에까지 관련 정보가 유출될 가능성도 제기되고 있어 사생활 침해 논란이 일었었다[76]. 금융위원회는 보험사기 조사를 위해 국민건강보험공단을 비롯한 관련 단체에 자료 제출을 요청하는 내용의 보험업법 개정안을 추진 중이라고 했

외, 전게서, 513면 : 김동규 외, 전게서, 128면.

76) 매일경제, 2008.7.31. A4면.

는데, 보건복지가족부는 사생활 보호를 이유로 이를 절대 허락할 수 없다는 입장이다. 사법기관도 제한적으로 접근하는 개인 질병정보를 민간 보험업계를 관리·감독하는 금융위원회가 열람하겠다는 것이라서 비판 의견이 많다. 이데 대해 금융위원회는 사기 우려가 있는 건에 대해서만 제한적으로 열람하겠다는 것이라 문제 될 것이 없다는 입장이다. 그러나 현행 형사소송법 등 질병정보를 활용할 근거가 있는데도 보험업법에 별도 규정을 두게 되면 오·남용 가능성이 많아질 것으로 생각된다. 특히 개인질병에 대한 공개가 시작되면 향후 의료정보가 민간보험회사로 넘어가는 것은 시간문제에 불과 할 것이다.

이와 같은 논란이 생기는 것도 근본적으로 현행 입법구조가 개인정보와 의료정보 보호가 각 개별법에서 제한적으로 다루어지고 있기 때문이라고 생각된다. 따라서 앞에서 본 바와 같이 개인정보는 물론 의료정보 보호를 위한 개별법의 입법이 이루어져야 체계적이고 종합적으로 정보보호의 길이 열리게 될 것이다. 금융위원회가 보험업법 개정을 시도하는 바로 이때가 관련법 입법의 최적기가 아닌가 생각한다.

앞서 살펴본 바와 같이 정보발전이 가속화 하면서 의료정보의 침해 가능성도 높아지지만, 상대적으로 발전되는 기술은 보안기술 역시 발전되어 침해에 대한 보호도 가능하게 될 것이다. 그렇지만 기술의 발전이나 제도적 보완 시스템을 갖춘다고 하더라도 관련되는 사람들의 도덕적 윤리적 책임감이 가장 중요하다고 생각한다. 왜냐하면 기술을 발전시키는 것이나, 법 제도를 만드는 것이나, 그러한 기술과 법적 제도적 관리체제를 이용 하는 것 모두가 그 바탕에는 사람이 있기 때문이다. 의료정보를 유출시키는 것도 사람이고, 그 결과에 대한 책임을 부담하는 것도 사람이다. 결국 사람이 문제이기도 하지만 해답이 되기도 하는 것이라고 생각한다.

〔 참 고 문 헌 〕

1. 단행본

강달천·김민섭, 김현철, 『2005년 개인정보 피해구제 및 상담사례분석』, 한국정보보호진흥원, 2005.12.

고영삼, 『전자감시사회와 프라이버시』, 한울 아카데미, 1998.

권건보, 『개인정보보호와 자기정보통제권』, 경인문화사, 2005.

국가정보원 (편저), 『국가정보보호백서』, 2006.

김동규·윤경일·박현애·한붕조·신현천·심영보, 『의료부분의 정보이용 활성화-초고속정보통신 기반구축 관련 법제도 정비안』, 한국보건사회연구원, 1995.

개인정보분쟁조정위원회, 『2004 개인정보분쟁조정사례집』, 한국정보보호진흥원, 2004.

백윤철·이창범·장교식, 『개인정보 보호법』, 한국학술정보, 2008.

한국정보보호진흥원 (편저), 『개인정보보호백서』, 한국정보보호진흥원, 2002.

_____, 『개인정보보호백서』, 한국정보보호진흥원, 2003.

2. 학술논문

공종렬, 「지식정보사회의 개인정보 침해사례분석과 보호정책에 관한 연구」, 박사학위논문, 경희대대학원, 2001.

김상찬, "의료정보의 제공에 관한 연구", 『일감법학』, 제8권, 2003.

김홍근·김윤정, 『지식정보사회 의료 패러다임 변화와 정보보안』, 한국정보보호진흥원, 2006.

길준규, "의료정보상 개인정보보호방안", 『법과 정책연구』, 제6집 제1호, 2006.

백윤철, "우리나라에서 의료정보와 개인정보보호", 『헌법학연구』, 제11권 제1호, 2005.

박정화, 「전자의무기록의 활용과 의료정보 보호방안에 관한 연구」, 석사학위논문, 연세대대학원, 2005.

오상원, "의사의 직업비밀 유지보호와 정보보호", 『법학연구』, 4권, 홍익대학교 법학연구소, 2002.

유지원, 「진료정보의 개인정보보호에 대한 의료인과 환자의 인식도 비교」, 석사학위논문, 고려대보건대학원, 2006

이미영·박영임, “간호사의 환자 프라이버시 보호행동에 대한 인식과 실천”, 『임상간호연구』, 제11권 제1호, 2005.

이부하, “환자의 의료정보권”, 『한양법학』, 제17집, 2005.

이인영, “개정 의료법의 환자의 개인정보 보호규정에 관한 법리적 고찰”, 『한림법학 Forum』, 제11권, 2002.

이창범, “생체프라이버시보호 원책에 관한 연구”, 『인터넷법률』, 제31호, 2005.

이현주, 「EMR시스템하에서 환자 진료정보보호를 위한 사용자 관리방안 연구」, 서울대학교 대학원 석사학위 논문, 2006.

장석천, “의료정보보호와 민사법적문제”, 『법학연구』, 제28집, 2007.

전영주, “의료법상 의료정보 보호방안”, 『법학연구』, 제28집, 2007.

_____, 『의료정보와 개인정보보호』, 법학연구 제23집, 한국법학회

진태영, 「의학적 검사 및 의무기록과 관련된 사생활의 비밀보호」, 석사학위논문, 연세대보건대학원, 2003.

Issues on the Patient's Information Protection

Jeong Bu Gyun

Samsung Medical Center, Manager Legal affairs part

=ABSTRACT=

Medical information is one of significant private information that includes individual's own diverse information. Once opened, it exposes one's health condition and medical history to a third party, which could bring about serious troubles. On this account, the third parties are of much concerns about the information. If medical information collected through various routes is used with another purpose, other than the initial intention, it might cause serious results beyond one's control. Thus, it is essential to keep the information confidential.

Also, the discrimination based on the medical information ought to be banned because it is likely to happen that exposed information socially stigmatizes a person, being discriminated in a work place or a school when he/she is employed or gets an insurance.

In the current system, only medical institutions are responsible for protecting or securing medical records. Despite the information technology development and the increased interests in medical information, there are quite a few limitations in legal, technical, and administrative aspects. All kinds of organizations, involved in collecting and using the information, as well as medical institutions primarily producing and managing it should share the responsibilities.

Keywords : medical information, private information, health condition and medical history, medical institutions, information technology development, information confidential, medical records