개인의료정보보호에 관한 법적 연구

연세대학교

의료법윤리학협동과정

법 학 전 공

박 인 경

개인의료정보보호에 관한 법적 연구

지도 손 명 세 교수

이 논문을 석사학위 논문으로 제출함

2006년 12월 일

연세대학교
의료법윤리학협동과정
법 학 전 공
박 인 경

박인경의 석사 학위논문을 인준함

심사위원 _____인

심사위원 _____인

심사위원 _____인

연세대학교 대학원

2006년 12월 일

감사의 글

먼저 논문을 무사히 마칠 수 있도록 인도해 주신 하나님께 감사드립니다. 논문을 쓰는 내내 그 분이 참으로 박인경이라는 작은 존재를 편애하고 계신다는 사실을 새삼 느낄 수 있었습니다. 그래서 더욱 감사드리고 또한 한없이 작은 제 모습이 부끄럽게 느껴집니다. 다시 공부할 수 있는 기회를 주시고 너무나 좋은 사람들과 만나 인연을 맺을 수 있도록 축복하여 주심에 감사드립니다. 지난 2년여 동안의 경험과 배움은 제 인생에 있어 많은 생각을 할 수 있는 기회를 주었고 또 그만큼 많은 성장을 할 수 있었던 토대가 되었습니다.

해박한 지식과 격려로 연구의 방향을 인도해 주신 손명세 교수님과 언제나 인자한 미소로 마음의 안식처가 되어 주셨던 박길준 교수님, 그리고 바쁘신 와중에도 자신의 논문처럼 세심히 지도하고 인도해 주신 장병철 교수님께도 깊은 감사의 말씀을 드리고, 제가 개인의료정보에 대하여 관심을 갖게 되는 계기를 만들어 주셨던 이경환 교수님과 채영문 교수님께도 감사드립니다.

생각하면 언제나 눈물부터 차오르는 사랑하는 아빠와 엄마 그리고 혼자서 고생하고 있을 내 동생 병천이... 논문 쓴다고 바쁘다는 핑계로 무심하기만 했지만 너무나 사랑하고 이 세상 어딘가에 존재한다는 것만으로도 힘이 됩니다. 한없이 순수한 눈동자로 항상 곁에 있어 주었던 사랑하는 마루와 항상 자신을 돌아보고 반성하게 해주는 등대같은 현희 언니 그리고 친언니같은 10년 지기 정화언니, 공부하느라 힘든데 논문 쓴다고 마음 써주지도 못해서 항상 미안한 정은이와 제대할 때까지 결국 위문편지 한통 보내지 못해 더 미안한 욱이, 짜증 다 받아주며 힘내라고 늘 맛있는 음식으로 사육해 주

었던 재관오빠, 멀리 호주에서도 힘이 되어 주셨던 종환 선생님과 너무나 이쁘고 좋아하는 윤희선생님, 차분함과 현명함으로 마음의 기둥이 되어 주셨던 현경선생님, 덩치만큼이나 넓은 마음으로 항상 웃음을 주는 현귀씨와 연애하느라고 바쁜 우민 형과 쿨가이 재현 형, 청주에서 깨소금을 볶고 있는 새색시 숙이 모두 고맙고 사랑합니다.

마지막으로 논문을 쓸 때까지 바쁜 사무실 업무에도 불구하고 이해하고 배려해 주신 이일학 선생님, 이은영 선생님을 비롯한 의료법윤리학과의 여러 선·후배님들과 설문에 자기 일처럼 성심껏 대답해 주신 각 병원의 여러 선생님들께도 다시 한번 감사의 말씀을 드립니다.

너무나 좋은 분들을 만나게 해 주신 하나님께 감사드리고, 사랑하는 사람들 앞에서 부끄럽지 않은 모습으로 살아가도록 언제나 노력하겠습니다.

박 인 경 올림

목 차

표 목차

그림 목차

국문 요약

개인의료정보는 의료인들이 환자에 대한 의료행위를 하면서 수집된 자료들과 이 자료들을 기초로 하여 연구 분석된 정보들을 포괄하는 것으로서 환자와 보건의료공급자로부터 수집되는 장기적이고 포괄적인 측면의 모든 정보의 집합을 의미한다. 이러한 의료정보는 보건의료정보화 및 인구·질병 구조의 변화와 같은 급변하는 보건의료환경에 적절히 대처하기 위하여 그 공유 및 활용의 필요성이 나날이 높아지고 있다. 그러나 의료정보와 같이 그 자체로서 내밀한 영역을 드러내는 민감한 개인정보는 그 수집 및 보유만으로도 인격 침해의 가능성이 크며, 그 성격상 일단 침해되어 버리면 회복이 곤란하기 때문에 특별히 강화된 보호가 요구됨은 주지의 사실이다.

우리나라는 의료관련 법령을 통해 의료정보보호에 관한 다수의 규정을 두고는 있지만, 의료정보의 특수성과 공익성을 고려한 종합적이고 구체적인 의료정보보호규정이나 의료정보보호와 보안에서 요구되는 내용을 충실히 포함하는 지침이 없어 그 보호가 상당히 미흡한 실정이다. 따라서 기본적으로 개인에 관한 정보이기 때문에 사생활의 비밀유지권의 대상이 되는 의료정보를 적절히 보호하는 한편, 개인정보통제권을 바탕으로 공적 성격을 지니는 의료정보의 이용을 통한 효용을 창출케 하면서 적극적으로 자기정보에 대한 흐름을 감시 및 통제하도록 하는 종합적이고 구체적인 제도의 마련이 요구되고 있다.

이 논문에서는 위와 같은 문제의식에 기초하여 제2장에서 개인정보로서의 의료정보 보호의 법적 의미와 내용을 분석하기 위하여 개인정보 및 개인정보보호의 헌법적 함의를 살핀 후, 의료정보의 개념 및 의료정보와 헌법적 기본권인 개인정보통제권과의 관계를 이론적으로 고찰하였다. 즉, 공익성과

사생활적인 성격을 모두 갖고 있는 의료정보는 그 이용과 보호를 동시에 추구하기 위하여 헌법상 개인정보통제권을 통하여 보호받아야 하며, 이러한 개인정보통제권은 의료정보주체 및 의료정보취급자에게 일정한 권리와 의무를 부과한다.

제3장에서는 의료정보의 활용과 보호라는 상반되는 이익을 동시에 충족시키기 위해서 필요한 의료정보보호의 전제가 되는 기준 및 원칙에 대해 살펴보기 위해 국외의 개인정보보호 및 의료정보보호제도를 살펴보았다.

제4장에서는 우리나라 의료정보보호제도를 고찰하기 위하여 국내의 의료정보보호법제 및 의료정보보호현황을 살펴보았다.

제5장에서는 앞에서 살펴 본 내용들을 바탕으로 도출된 의료정보의 주체별·단계별 쟁점 사항을 정리하고, 이를 중심으로 개선방안을 제시하였다.

우선, 의료정보주체는 의료정보의 흐름을 원칙적으로 정보주체의 의사에 따르도록 하기 위해 수집동의권 및 그 전제가 되는 설명청구권을 가지며, 정보의 수집은 명확한 목적과 적절한 범위 내에서 적절한 절차를 통한 충분한 설명을 제공한 후 사전 동의를 통해 이루어져야 한다. 둘째, 원칙적으로 의료정보주체 또는 지정대리인만이 자신의 의료정보에 대한 접근권을 가지며, 자기 정보의 오류에 대하여 일정부분 정정청구권을 가진다. 셋째, 의료정보주체는 정보 침해 단계에서 침해중단청구권, 추가적 동의권, 개시 고지권 등을 보장받아야 한다. 넷째, 의료정보취급자는 개인의료정보의 안전성을 확보하기 위한 보안유지방법으로 관리적, 물리적, 기술적, 사용 보안 장치를 강구해야 한다. 다섯째, 의료정보취급자는 기본적으로 개인의료정보보호를 위하여 최선을 다할 선량한 관리자의 의무를 가지며, 의료인 뿐 아니라 의료인이외의 내부정보취급자 또한 의료정보의 비밀유지 의무를 부담해야 한다. 여섯째, 의료정보를 처리 및 이용 또는 제3자에게 제공하는 경우, 치료·지불·의료업무관리와 같은 통상적인 사용의 경우에는 환자의 동의 없이도 그 목

적 범위 내에서 의료정보를 이용할 수 있다 할 것이지만 그 외의 이용 및 제공의 경우에는 원칙적으로 환자의 의사에 따라야 한다. 그러나 존재할 수 있는 다양한 혼란을 방지하기 위하여, 의료정보이용 및 제공에 대한 원칙 및 예외를 구분하여 상세히 규정할 필요가 있다.

제6장에서는 앞에서 살펴본 개인의료정보보호방안의 내용을 바탕으로 현재 입법이 진행 중인 건강정보보호를 위한 법률안들의 내용을 구체적으로 검토·분석하여 개선점을 제시하였다.

제**7**장에서는 이전까지 논의되었던 것을 토대로 결론을 맺음으로써 본 논문을 마무리하였다. 그 자체가 무한한 정보원으로서 효용성이 큰 의료정보는 의료정보화가 진행됨에 따라 그 이용 및 공유의 필요성이 더욱 증가할 것이며 그에 비례하여 그 침해의 가능성 또한 증가할 수밖에 없다. 이러한 우려에 따라 의료정보를 보호하기 위한 법률을 제정하고자 하는 움직임이 여기저기에서 일어나고 있지만, 조속한 입법을 위한 사회적인 합의가 쉽게 이루어지지 못하고 있는 실정이다. 따라서 의료의 질을 향상시키고 환자의 권리를 보호하기 위하여, 의료정보화라는 시대적인 요청과 조화를 이루는 사회·제도적인 장치를 마련하기 위한 노력을 기울여야 할 것이다.

핵심되는 말 : 의료정보, 건강정보, 개인의료정보보호, 개인정보통제권, HIPAA 프라이버시규칙

제1장 서 론

1.1 연구의 배경

1.1.1 지역보건의료정보화

현대 보건의료는 인구고령화 및 만성질환자의 증가[1] 등 과거와 비교할 수 없을 정도로 급속히 변화하는 보건 의료 환경에 직면하고 있다. 이러한 인구 및 질병구조의 변화는 필연적으로 국민의료비의 증가를 야기할 수밖에 없으며 이는 곧 국민 개개인의 경제적 부담 및 국가 재정의 낭비로 연결된다. 따라서 급속히 증가하고 있는 국민의료비 부담 증가를 막고 국민의 건강한 삶의 질을 보장하기 위하여 정부는 국가적 차원의 질병의 예방 및 관리체계를 구축하고 보건의료서비스간 기능 연계를 통한 국민의 생애주기별 보건의료서비스를 개발하고자 노력하고 있다. 각 지방에서 자체적으로 지역의 수요와 실정에 따라 지역보건의료정보화계획 등 보건사업 계획을 수립하여 이를 수행하는 한편, 중앙정부에서 이를 적절히 평가·지원토록 하는 것이 바로 그것이다. 이는 각 보건기관이 지역주민들의 의료정보를 데이터베이스화하여 보다 적극적으로 이를 축적·활용하며 국민건강보험공단 등 관계기관과 정보연계를 통한 다양한 통계 및 정책정보를 생산하여 활용하도록 하고자 하는 것이다.

그에 따른 정책의 일환으로 보건복지부에서는 전국 보건소의 진료 및 진료지원, 보건사업 등 업무의 전산화를 위하여 지난 1994년 지역보건의료

1) 우리나라 고령인구는 다른 나라에 비하여 급속히 증가하고 있어 2020년경에는 65세 인구가 14%에 이르는 고령사회로 진입할 예정이다. 또한 암, 고혈압, 당뇨병, 심장병 등의 만성질환과 사고에 의한 사망률이 1983년 58.5%에서 1995년 70%로 크게 증가하게 되었다. 김곤희, “우리나라 지역보건의료 EHR체계 구축 방안에 대한 연구”, 연세대 보건대학원 석사논문, 1면

전산화사업을 추진, 1997년부터 보건소표준정보시스템을 개발·확산하였으며, 2005년 전국 246개 보건소 및 보건의료원 중 11개소를 제외한 95.5%(235개소)에 해당하는 보건소 및 보건의료원에 정보 시스템을 설치하였다. 특히 2004년도에는 주민이 타 보건소로 이동할 경우, 타 보건소에서 환자의 동의 하에 기존 보건소의 환자 진료내역을 참조할 수 있도록 보건소간 주민보건정보 공동 활용 시스템[2]을 개발하여 사용하고 있다. 그러나 2005년 "지역보건의료분야 정보화전략계획수립 사업"의 조사 결과, 보건소간 주민보건정보 공동 활용 시스템은 환자의 개인정보의 보안·관리가 미흡하고 정보시스템의 유지관리 및 교육, help 지원이 미흡하다는 문제점[3]을 안고 있어 이에 대한 대책이 필요한 실정[4]이다.

1.1.2 보건의료정보화

전자정부를 비롯한 사회 각 부문의 정보화가 진전됨에 따라 건강보험

---

2) 동 시스템의 주민정보 공동 활용 절차는 다음과 같다. 현재 보건기관의 실무자가 주민과 함께 보건사업 및 진료를 과거 주민이 서비스를 받았던 보건기관에 보관된 정보가 필요할 때 업무담당자는 주민의 동의를 얻고 정해진 서식에 따라 상위 결재권자의 결재를 거쳐 해당 보건기관에 정보전달 요청을 한다. 정보전달 요청을 받은 보건정보관리 담당자는 소속 보건기관의 DB를 검색하여 해당 정보를 확인하고, 소속 상급자의 결재를 거쳐 요청 보건기관으로 전송한다. 이 과정 또한 행정전자서명에 의한 인증절차를 거쳐야 한다. 김곤희, 앞의 논문, 15면

3) 그 밖에도 보건소간 주민보건정보 공동 활용 시스템은 "첫째, 보건기관 단위로 환자의 진료기록을 생성·보관하고 관리함으로써 지역주민이 타 보건소로 전출시 마다 주민의 데이터가 중복적으로 생성·관리되고 있으며, 소속되는 지역의 보건소가 아닌 타 보건소에서 보건서비스를 받기 어렵다. 둘째, 관련 행정기관인 시·도 보건과, 보건복지부, 질병관리본부 등과의 수직적인 정보교류체계가 구축되어 있지 않아 각종 보고통계 등 이중 보고하는 사례 등으로 업무의 능률이 낮다. 셋째, 보건소간, 그리고 공공의료기관 등 관련기관과 수평적인 정보교류 체계가 구축되어 있지 않아, 연속진료 등 이용자에게 유용한 정보서비스를 제공하지 못하고 있다. 넷째, 각종 보건사업간 관련 DB가 연동되지 않아 중복적으로 접수, 관리되고 있으며, 기능의 미약으로 수기작업이 너무 많아 오류가 많이 발생하고 있다. 다섯째, 보건정보를 가공·활용한 CRM(고객관계관리)서비스 및 홈페이지를 통한 대민서비스 제공 기능이 전혀 없다." 등의 문제점을 안고 있어 현재 제도적인 개선 도상에 있는 실정이다.

4) 김곤희, "우리나라 지역보건의료 EHR체계 구축 방안에 대한 연구", 연세대 보건대학원 석사논문, 16면, 보건복지부, "지역보건의료분야 정보화전략계획 수립 중간보고서", 2005

을 비롯한 4대 사회보험의 정보연계가 이루어지고 있으며, 의료부분에서는 국가적으로 2010년까지 전국민 전자건강기록 시스템을 구축하여, 의료기관 간의 진료정보를 공동으로 활용하게 함으로써 의료서비스의 질을 향상시킴과 동시에 편리하고 효율적인 의료서비스를 보장하고자 하는 의료정보화계획이 추진 중이다. 이를 위해 보건복지부에서는 1998년에 수립한 21세기 보건의료 발전 종합계획에 국가보건복지정보화계획을 포함시키는 한편 의료의 선진화를 위한 4대 기본목표[5]를 설정하고 환자의 평생 전자건강기록 체계를 구축하기 위한 정책을 추진·수행하고 있다. 또한 2004년도에는 보건의료분야 정보화 시행계획을 통해 진료정보 공동 활용을 위한 기반을 조성함으로써 진료정보 공유내용(컨텐츠), 진료정보공유 전산기술 및 진료정보공유 활성화를 위한 기반을 조성해 내는 성과를 이룬 상태[6]이다. 그러나 환자 개인정보 보호 및 의료정보시스템의 보안 기준 등에 대한 구체적인 연구가 미흡한 현 상황에서는 개인정보의 부적절한 사용 등 의료정보 침해로 인해 보건의료의 정보화가 가져다 줄 긍정적 파급효과를 감소시키는 결과를 초래할 수도 있다는 점을 간과할 수 없다. 보건의료정보화는 정보의 공유와 활용이라는 측면의 중요성과 동시에 환자의 개인정보에 대한 침해 가능성이라는 양날의 칼을 항상 가지고 있다. 의료정보의 정보화가 진행되면 필연적으로 정보에 대한 무분별하고 광범위한 접근이 가능해지게 되게 되고, 이에 따라 정보에 대한 침해의 가능성도 증가하기 때문이다. 더욱이 의료정보는 개인의 생명·신체와 직결된 사항이기에 그 보호의 필요성은 더욱 크다 할 것임에도 불구하고 국내 의료정보보호의 중요성에 대한 인식은 정보화 수준에 미치지 못하고 있는 실정이며, 이를 뒷받침해 줄 공공기관과

---

5) 첫째, 평생국민건강관리체계구축
둘째, 수요자 중심의 보건의료공급체계 구축
셋째, 보건의료산업의 경쟁력 제고
넷째, 보건의료 선진화의 기반 조성

6) 한국보건산업진흥원, "국가보건의료정보화계획(안)", 2005

민간기관을 아우르는 종합적이고 구체적인 보호방안도 미흡하여 많은 혼란을 야기하고 있다.

1.2 연구의 목적

경제수준이 향상되고 정보통신기술이 눈부시게 발전해 나감에 따라 보건의료서비스의 질에 대한 국민들의 기대도 꾸준히 증가하고 있다. 이에 발맞추어 의료소비자 중심의 보건의료, 신속한 안방민원서비스, 맞춤형 환자관리 등 환자와 의료인 양자 모두의 편의성과 만족도를 향상하기 위하여 환자들의 의료정보를 집적하고 전산화하며, 필요시 병원 간에 공유하는 보건의료정보화계획이 활발히 추진 중임은 주지의 사실이다. 뿐만 아니라 빠르게 발전하는 정보화에 대응하고 환자 중심의 의료서비스를 추구하기 위하여서도 의료정보는 개인의 안녕과 공공의 목적을 위해 공동으로 활용되어야만 할 개연성이 크다. 그러나 이러한 보건의료정보화를 통한 의료정보의 활용은 환자의 인적 사항이나, 병력, 치료과정, 투입 약물 등 민감할 수밖에 없는 개인정보들이 전산화되어 집적될 수 있기 때문에 의료정보의 공유 및 활용이 증가하게 될수록 이에 비례하여 개인의 정보 인권 침해에 대한 우려 또한 증가하는 것이 사실이다. 특히 개인의료정보들이 집적되는 경우, 해킹이나 바이러스 침투로 정보가 손실되거나 개인정보가 대량으로 유출될 수 있는 가능성을 배제할 수 없으며 집적된 방대한 국민의 의료정보가 상업적인 목적으로 유출될 경우 그 피해는 고스란히 국민에게 돌아갈 수밖에 없기 때문이다. 따라서 의료정보의 공유 및 활용성이 증가하는 것과 비례하여 의료정보보호를 위한 법적·기술적 장치를 마련하는 것의 중요성은 아무리 강조해도 지나치지 않다. 그러나 의료정보보호라는 미명 하에 의료정보의 공유 및 활용을 억제하는 폐쇄적인 관리 또한 정보화 시대

의 흐름에 거스르는 일임에 틀림없다. 본 연구에서는 개인의료정보보호의 법적 성격을 분석하는 한편, 국·내외의 의료정보화에 따른 의료정보보호 현황 및 제도를 조사·분석함으로써 의료정보보호의 쟁점사항을 도출하고 현재 진행 중인 건강정보보호를 위한 법률안의 내용을 분석하여 의료기관을 비롯한 각 보건의료계가 정보화라는 급격한 환경변화에 대처할 수 있도록 의료정보의 활용과 조화를 이루는 개인의료정보보호 방안을 제시하는데 그 목적이 있다. 이는 국민의 알권리 및 의료정보통제권 등 의료정보인권을 보호하는 한편, 건강한 보건의료정보화 및 의료정보 공동 활용 구축에 이바지함으로써 의료체계의 효율성을 향상시켜 궁극적으로 국민의 삶의 질을 보다 향상시킬 것으로 기대한다.

1.3 연구의 범위 및 방법

본 연구는 개인의료정보보호의 법적 개념 및 의의를 고찰함과 동시에 의료정보주체 및 의료정보취급자의 권리·의무 및 의료정보처리과정에 따른 주요 쟁점사항을 분석하고, 국·내외 의료정보의 보호 법제도 및 현황을 살펴봄으로써 이러한 과정에서 도출된 쟁점사항과 원칙을 토대로 보건의료정보화 및 의료정보 활용이라는 시대적인 요청과 조화를 이루는 개인의료정보보호방안을 제시하고자 하는 것이다. 따라서 기본적으로 현재 실시되고 있는 개인의료정보보호에 관한 국내·외의 관련 법제가 기본적인 연구 범위가 된다.

우선 제2장에서는 개인정보로서의 의료정보의 법적인 의미를 살펴보고, 의료정보보호와 헌법상 기본권인 개인정보통제권과의 관계를 법이론적으로 고찰하여 의료정보에 있어 개인정보통제권을 구체적으로 실현하기 위한 주체별·단계별 쟁점사항을 도출하고자 한다.

제3장에서는 의료정보보호의 전제가 되는 기준 및 원칙에 대해 살펴보기 위해 국외의 개인정보보호 및 의료정보보호제도를 살펴보고자 한다.

제4장에서는 국내의 의료정보보호 관련 법제를 고찰하는 한편 현재 대형 병원들의 구체적인 의료정보보호현황을 조사·분석해 보고자 한다.

제5장에서는 앞에서 고찰한 내용들을 토대로 도출된 의료정보의 주체별·단계별 법적 쟁점 사항을 논의하고, 이를 중심으로 종합적이고 구체적인 개인의료정보보호방안을 살펴보고자 한다.

제6장에서는 앞에서 살펴본 개인의료정보보호방안의 내용을 바탕으로 현재 입법이 진행 중인 건강정보보호를 위한 법률안들의 내용을 구체적으로 검토·분석하여 개선점을 제시한다.

본 논문에서는 우리나라의 의료정보보호를 위한 쟁점사항을 도출하고 이에 대한 개선방안을 살펴보기 위해서 각국의 법제들을 비교법적으로 검토해 보았다. 특히 미국의 HIPAA 프라이버시규칙, OECD 개인정보보호 가이드라인과 현재 입법이 진행 중인 건강정보보호 및 관리·운영에 관한 법률안 등의 관련 법규 및 국내·외의 관련 저서와 논문 그리고 인터넷 사이트 정보 및 보도 자료를 기초로 하는 문헌적 연구방법을 채택하였다. 그 밖에 몇몇의 대형 병원들을 직접 대상으로 하여 의료정보보호 현황을 간단히 구두 또는 서면질의를 통해 조사하였다.

제2장 개인의료정보의 보호

2.1 개인정보보호

2.1.1 개인정보

2.1.1.1 개인정보의 의미

인간은 혼자서 살아갈 수 없는 사회적 동물이다. 따라서 필연적으로 사회생활을 하는 과정에서 여러 가지 사실들이 생겨나고 이러한 사실들은 의도하건 의도하지 않건 기록 또는 자료로 남아 수집 및 저장 이용되게 된다. 이러한 기록 및 자료 가운데 특히 개인에 관한 기록이 수집 및 저장되어 정보의 형태를 취하는 것이 개인에 관한 정보라고 할 수 있다.

우리나라의 경우 여러 법률[7]에서 개인정보에 대한 정의를 내리고 있는데, 공공기관의 개인정보보호에 관한 법률은 개인정보를 제2조 제2호에서 "생존하는 개인에 관한 정보로서, 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없다 하더라도, 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"로 정의하고 있다.

이러한 개인정보의 개념[8]은 개인의 정신, 신체, 재산, 사회적 지위, 신

---

7) 정보통신망이용촉진및정보보호등에관한법률에서도 개인정보를 "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 경우에는 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"로 정의하고 있고 있으며(제2조 제1항 제6호), 전자서명법에서도 "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)"로 정의하고 있다(제2조 제13호).

분 등에 관한 사실·판단·평가를 나타내는 일체의 정보가 포함되는데, 개인 식별이 가능한 정보로는 내면의 비밀(사상, 신조, 종교, 가치관, 양심 등)과 심신의 상태(체력, 건강상태, 신체적 특징, 병력 등), 사회경력(학력, 범죄경력, 직업, 자격, 소속정당, 단체 등), 경제관계(재산상황, 소득, 채권·채무관계 등), 생활·가정·신분관계(성명, 주소, 본적, 가족관계, 출생지, 본관 등)로 구체화할 수 있다.

위와 같은 정의에 비추어 개념을 정립하여 보면 개인정보는 생존하는 자연인의 내면적 사실, 신체나 재산상의 특질, 사회적 지위나 속성에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체를 일컫는 것으로 이해할 수 있다. 따라서 생존하고 있는 개인의 가족 병력기록, 과거의 의료기록, 신체장애, 혈액형, 유전정보 등의 의료정보가 개인을 식별하거나 식별할 수 있는 정보의 총체로 존재할 경우 그것은 '개인정보'로서의 의료정보인 것이다.

8) 권건보, "개인정보보호와 자기정보통제권", 경인문화사, 2005, 14면

2.1.1.2 개인정보의 분류

개인정보는 먼저 식별가능성에 따라 직접식별개인정보와 간접식별개인정보 및 익명정보로 분류[9]할 수 있다.

직접식별개인정보란 성명, 지문, 주민등록번호, 운전면허번호, 신용카드번호 등과 같이 그 정보 자체에 의해서 특정인의 신원을 직접 식별하거나 식별할 수 있는 정보를 말한다. 반면, 간접식별개인정보는 주소, 전화번호, 성별, 가족관계, 신장, 병력, 경력, 학력 등과 같이 그 정보만으로는 특정인의 신원을 식별할 수 없지만 다른 정보와 결합하게되면 특정인을 식별하거나 식별할 수 있는 정보를 말한다. 익명정보란 특정 개인과 정보를 연결할 합리적인 수단이 전혀 없는 것으로서, 모든 식별자를 삭제한 정보를 말한다. 대부분의 이러한 익명정보의 경우 사생활 침해의 가능성은 존재하지 않는다고 추정되나 이점에 대하여는 논의의 여지가 있는 것으로 보인다.[10]

또한 개인정보는 보호의 필요성 정도에 따라 절대적 개인정보와 상대적 개인정보로 분류할 수도 있다. 즉, 절대적 개인정보[11]란 그 정보의 공개를 절대적으로 제한할 필요성이 있어 가장 강력한 보호가 요구되는 정보로서 DNA정보, 성적 특성, 혈통, 건강 및 의료기록, 신조나 양심의 주관적 가치와 같은 내면의 정보가 이에 해당된다. 이에 반하여 상대적 개인정보란 법령의 규정이나 계약 또는 행정기관의 직권에 의해서 공개나 사용이

---

9) 권건보, 위의 책, 25면

10) 그러나 의료정보의 경우 개인정보의 개념을 단순히 식별하거나 식별할 수 있는 정보의 총체로 한정시킬 경우 보호 영역 밖의 문제가 발생될 수 있다는 문제점이 있다. 예컨대 환자의 동의없이 환자의 얼굴만을 삭제한 채 공개되는 신체 노출 사진 등이 마케팅이나 재판의 증거자료로 사용되는 경우가 그러하다. 따라서 의료정보보호의 이익이 있는 개인의료정보의 개념이란 정보주체인 환자가 타인에게 알리고 싶지 않다고 생각하는 것이 정당한 일정한 이익이 존재하는 사적인 영역으로서 논의할 필요가 있다.

11) 이러한 정보는 민감한 정보라고 불리기도 한다.

가능한 개인정보를 말한다. 이는 어떤 개인정보를 어느 정도로 보호할 것인가 하는 실천적 문제에 대한 해법의 하나로서 제시되고 있는 구분법이다[12].

이러한 개인정보로서의 의료정보를 앞서 제시한 두 가지 분류 방법에 따라 나누어 보면 의료정보에 대한 분류도 가능해지며, 이는 의료정보의 활용을 위한 구체적인 보호의 기준에 대한 실마리를 제시한다.

2.1.2 개인정보보호의 헌법적 고찰

2.1.2.1 개인정보보호의 전통적 고찰

개인정보보호 문제는 일반적으로 헌법적 기본권으로서의 프라이버시권이나 사생활보호권[13]의 재구성이라는 개념으로 포괄하여 접근하는 것이 주류이다. 이러한 헌법상 프라이버시권은 국가로부터 사생활을 침해당하지 않을 소극적인 권리로 이해되다가, 정보사회인 현대에 들어와 기존의 소극적 권리뿐만 아니라 개인정보에 대하여 자기가 결정할 수 있는 적극적 권리로까지 발전하였다[14]. 이 견해에 의하면 개인정보보호에 대한 논의는 사생활의 내용을 공개 당하지 아니할 권리, 사생활의 자유로운 형성과 전개를 방해받지 아니할 권리와 자신에 관한 정보를 통제할 수 있는 권리(정보의 프라이버시 혹은 개인정보통제권) 등을 포함하는 사생활 보호권에 바탕한 프라이버시권[15]의 영역에서 논하게 된다. 그러나 이러한 접근은 개인정

12) 권건보, "개인정보보호와 개인정보통제권", 경인문화사, 2005, 19면
13) 허영, "헌법이론과 헌법", 박영사, 2006, 502-506면
14) 남효순, "인터넷과 법률", 법문사, 2005, 459-466면
15) 김종철 교수의 견해에 의하면 소극적 프라이버시권뿐 아니라 적극적 프라이버시개념도 개인의 정치적 의사형성과 사회적 자율성의 전제로서 기본적으로 사적 성격의 개인정보를 보호하여야 한다는 발상에 의거하고 있으므로 그 기본전제가 사생활보호에 천착하고 있다는 점에서 소극적 프라이버시와 동일하다고 한다. 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론",인터넷

보보호를 프라이버시라는 사적 영역에 한정하여 고찰하게 되는 결과 개인정보의 운용과 보호가 가지는 공적인 측면을 간과하게 되는 경향이 있었다. 뿐만 아니라 개인정보보호의 정당성을 개인의 인격성의 보호나 자율성의 보호라는 사생활영역의 보장에 한정시킴으로써 일상화된 정보관리에 대한 적극적 통제나 정치 및 경제 권력에 대한 견제권으로서의 정치적, 헌법적 의미를 담보하기에는 미흡하다는 한계를 가졌다.[16)]

2.1.2.2 개인정보보호의 현대적 고찰

사생활 보호 차원에서의 개인정보란 절대적으로 보호되는 것이 아니며 그 경계도 정치과정을 통해 재조정되는 유동적인 것이다.[17)] 공동체의 운영과 직접적으로 관련이 없는 정보의 경우는 개인의 인격 보호라는 전통적인 사생활 보호 차원에서 계속 프라이버시권의 보호를 받는다. 그러나 공동체의 운영상의 필요에 의해 혹은 기타 사회적 필요에 의해 행해지는 일정 개인정보의 수집 및 활용은 적법한 절차에 의하는 한 허용되어야 한다. 다만, 이 과정에서 반드시 이 수집된 정보가 오, 남용되는 것을 통제하는 절차적이고 실체적인 권리를 정보의 주체인 개인에게 인정할 필요가 있다는 것이다. 즉, 단순히 사생활 보호 영역에서 취급되던 전통적 개념으로부터 분리된 새로운 개인정보통제권은 자신의 정보가 어떻게 수집, 처리, 관리, 이용되는지에 대한 감독권을 의미한다. 이 권리는 적극적 프라이버시권의 개념 하에 보호되던 정보에의 접근권과 정보수정 및 삭제권을 그 내용으로 포섭할 뿐 아니라 이 정보가 원래의 목적 달성을 위해서만 사용되고 있는

법률 4호2001.1. 36면

16) 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론",인터넷법률 4호2001.1. 36면

17) A.Etzioni, The Limits of Privacy, Basic Books, 1999

지에 대한 감독권까지 포함하는 것이다.[18] 따라서 현대적 의미의 개인정보 통제권의 대상인 개인정보는 소극적 방어권으로서의 사생활의 비밀유지권의 보호대상이 되는 한편 이 정보에 대한 지속적인 접근권과 정보의 정확성을 확보하는 적극적 권리행사의 대상이 된 것이다.

2.1.2.3 개인정보통제권의 내용

헌법상 기본권인 개인정보통제권은 적극적 프라이버시권의 개념 하에 보호되던 정보에의 접근권과 정보수정, 삭제권을 그 내용으로 포섭할 뿐 아니라 이 정보가 원래의 목적 달성을 위해서만 사용되고 있는지에 대한 감독권까지 포함하게 된다. 즉, 개인정보통제권은 타인에게 알리고 싶지 않다고 생각하는 것이 정당한 일정한 사적인 개인정보에 관하여 개인정보의 수집 및 획득, 개인정보의 보유 및 이용, 개인정보의 열람 및 제공의 각각의 단계에서 정보주체에 의한 통제의 권리보장을 요구함과 동시에 이러한 권리를 실효적으로 확보하기 위하여 개인정보의 열람청구권 및 정정청구권을 도출하며 나아가 정보취급자에게 정보수집의 목적 이외에 사용하지 않거나 정보보안에 철저할 것을 요구할 수 있을 뿐 아니라 이용 및 제공 통제권의 보장을 요구한다[19].

2.1.2.4 개인정보통제권의 제한

헌법상 권리인 개인정보통제권이 절대적으로 보호되는 권리가 아니며,

---

18) 강경근교수는 정보프라이버시와 정보보안을 개념적으로 구분하여야 디지털시대 정보화가 개인의 이익신장뿐만 아니라 공동체 가치실현에도 기여할 수 있다고 적절히 지적하고 있다. (강경선, "사이버스페이스에서의 기본권", 헌법학연구 제6권 제3호, 17-18면)
19) 권건보, 위의 책, 34면

국가의 안전보장, 질서유지 및 공공복리를 위하여 제한될 수 있는 권리임은 주지의 사실이다. 개인정보통제권의 제한을 합법화하는 기준인 비례 원칙의 일반적 내용[20]은 다음과 같다.

첫째, 목적의 정당성이다. 즉 개인정보통제권을 제한하려는 목적이 정당하여야 한다. 따라서 정보주체의 동의에 의하지 않은 개인정보의 수집이나 열람거부, 목적 외 이용, 대외적 공표 등이 국가안전보장 질서유지 또는 공공복리를 위해서 이루어지거나 허용되는 경우에만 그 목적의 정당성이 인정될 수 있을 것이다[21].

둘째, 개인정보통제권을 제한하는 조치가 목적을 달성하는데 적합한 수단이어야 한다. 따라서 개인정보의 수집과 처리는 추구하는 목적을 달성하는데 효과적인 수단일 것이 요구된다. 그러나 만일 개인정보의 비밀수집이 공개 등의 조치를 취하더라도 해당 목적을 달성하는 데는 별다른 효과를 기대하기 어려운 경우라면 수단의 적합성은 인정될 수 없을 것이다.

셋째, 해당 목적을 위한 경우라도 필요 최소한의 정보처리가 요구된다. 공권력에 의한 개인정보의 처리는 명백하고 정당한 공적 과제의 이행이라는 목적에 기여하는 경우라 하더라도 이러한 목적을 달성하는데 있어서 적합한 방식으로 필요한 최소한으로 이루어져야[22] 한다.

넷째, 개인정보통제권의 제한이 불가피하고 최소한으로 이루어지는 경우라 하더라도 법익의 균형성이 요청된다. 즉 개인정보통제권의 제한으로 인한 피해의 이익이 그 제한을 통하여 달성하고자 하는 공익보다 적어야만 정당한 기본권제한이 될 수 있다. 보호이익과 피해이익 사이의 형량에 있어서는 개인정보에 대한 침해의 성질, 강도, 민감성 등이 고려되어야 할 것이다.

---

20) 남효순, "인터넷과 법률", 법문사, 2005, 150면
21) 김철수, " 헌법학개론", 박영사, 2006, 349면
22) 허영, "한국헌법론", 박영사, 2006, 283면

한편 아무리 긴요한 공익을 위한 경우라고 할지라도 정보주체를 단순한 정보의 객체로 전락시키는 결과를 초래한다면 그것은 개인정보통제권의 본질적 내용의 침해[23]가 될 것이다.

2.1.2.5 개인정보통제권의 침해 유형

(1) 위법·부당한 수집에 의한 침해

국가 및 공공기관 등은 국가안전보장·질서유지 및 공공복리 등 일정한 목적을 수행하기 위하여 개인정보를 수집할 필요성이 있는 경우 목적달성에 필요한 한도 내에서 개인정보를 수집하여야 한다.[24] 그러나 이러한 원칙에도 불구하고 목적달성의 한계를 넘어서 개인정보를 수집하는 경우나 개인정보를 개인의 참여 없이 비밀리에 수집하는 경우도 있다. 이와 같이 개인정보는 ① 목적달성 또는 업무상 필요한 한도를 벗어난 수집, ② 본인의 동의가 없는 수집, ③ 위법 또는 부당한 수단에 의한 수집[25] 등에 의하여 침해될 수 있다.

(2) 이용목적 이외의 목적으로의 이용에 의한 침해

수집된 개인정보는 명확하게 표시된 목적 이외의 목적으로 이용되어서는 안 된다. 따라서 수집·이용목적 이외의 목적으로 개인정보가 이용되는 경우에 개인정보는 침해된다. 이것이 개인정보침해유형 중 가장 문제되는 유형이다. 개인정보는 각 기관 상호간에 교환되거나 공동 활용되게 될 경우 즉 정보에 대한 접근가능성이 확대될수록 본래의 수집목적 이외의 목적

23) 허영, 위의 책, 269면, 282면
24) 권건보, 위의 책, 116면
25) 위법·부당한 수단에 의한 수집에는 개인정보 수집 시 고지 및 명시의무를 이행하지 않는 행위가 포함된다. 김철수, 위의 책, 344-348면

으로 이용될 가능성이 증가한다. 이는 특히 전자정부 및 보건의료정보화 등으로 인하여 개인정보가 공동 이용되는 경우에 침해가능성이 더욱 증대된다. 따라서 개인정보는 ① 수집목적 이외의 이용 및 제공, ② 본인에게 불이익한 이용 및 제공 등에 의하여 침해될 수 있다.

(3) 개인정보의 부정확성 등에 의한 침해

개인의 정보는 목적에 필요한 범위 내에서 정확하고 최신의 것이어야 한다. 즉 부정확한 정보, 잘못된 과거의 정보 등에 의하여 정보주체의 권익이 침해되게 된다. 즉 잘못된 정보의 입력으로 성병환자나 전염병환자로 오인되는 경우 등이 이에 해당한다. 한번 수집된 정보는 정보주체에게 오류를 수정할 기회를 부여하지 않는 한 잘못된 정보의 상태로 이용되게 된다. 그러므로 정보주체에게 정보열람청구권, 정정청구권 등이 인정되어야 하는 것이다. 따라서 개인정보는 ① 본래의 목적이외의 목적을 위한 유지·관리 ② 잘못된 정보의 유지·관리 등에 의하여 침해된다.

(4) 개인정보의 유출·변조 등에 의한 침해

정보통신의 발달로 인해 정당한 권한이 없는 자 또는 정보를 처리하는 담당자가 부당하게 개인정보를 변조·가공할 위험성이 증가되었으며, 또한 개인정보를 외부에 유출하여 정보주체에게 막대한 불이익을 주는 사건도 발생하고 있다. 따라서 개인정보는 ① 부당한 개인정보의 변조·유출 등에 대한 안전대책의 결여 ② 외부위탁 시의 보호조치의 결여 등에 의하여 침해될 수 있다.

위와 같이 개인정보통제권의 침해 유형을 구분하는 것은 개인정보의 성질상 한번 침해되면 원상회복이 용이하지 않다는 점과 맞물려 그 의미를

갖게 된다. 즉, 침해 유형을 구체화하여 사전에 침해를 방지할 수 있는 방안을 마련 및 보장하는 것이 가장 헌법적·국민적·시대적 요청에 부응하는 것이기 때문이다.

2.1.3 개인정보보호의 의의

개인정보통제권이 권리로 인정된다고 하는 것은 권리침해에 대하여 법원에 소송을 제기하여 구제를 요청할 수 있다는 것을 의미한다는 점에서 상당히 고무적인 일이다. 그러나 개인정보는 그 성격상 일단 침해되어 버리면 원상을 회복하는 것이 상당히 곤란하다. 따라서 개인정보를 진정으로 보호하기 위해서는 권리가 침해되지 않도록 사전에 보호조치를 취해야한다. 또한 개인정보통제권의 대상인 타인에게 알리고 싶지 않다고 생각하는 것이 정당한 사적인 개인정보의 범위는 미묘할 뿐만 아니라 일일이 열거하는 것 또한 불가능하다. 그러한 까닭에 개인정보통제권의 침해라고까지는 말 할 수 없어도, 개인정보에 관하여 보호조치를 취하는 것이 법·정책적으로 중요하다. 그리하여 요구되는 것이 개인정보보호제도이다.

특히 현대사회와 같이 정보화 사회가 되어 컴퓨터로 대량의 개인정보가 집적되고, 대량의 정보가 순식간에 송신되는 시대에 있어서는 이러한 개인정보보호의 필요성은 더욱 절실하다. 미국이나 유럽에서 프라이버시보호나 개인정보보호의 조치를 취하고 있는 것은 그 때문이라고 할 것이다. 한국도 물론 예외는 아니다. 그런 까닭에 한국에서도 신속하게 개인정보보호의 법제를 정비할 필요성이 크다.

2.2 의료정보의 보호

2.2.1 의료정보

2.2.1.1 의료정보의 개념

의료정보는 개인정보의 일종으로서 개인정보통제권의 보호대상이다. 좁은 의미의 의료정보[26]라 함은 의사가 환자에 대한 의료행위를 하면서 수집된 자료들과 이 자료들을 기초로 하여 연구 분석된 정보들을 포괄하는 것으로서 진단과 그에 따른 치료행위, 치료경과에 따른 면밀한 관찰 등을 모두 포함하는 전체과정에서 수집된 자료들을 의미[27]한다. 그러나 본 연구의 대상이 되는 의료정보는 다음의 그림과 같이 좁은 의미의 의료정보를 포함하는 개인의 전 생애에 걸쳐서 환자와 보건의료공급자로부터 수집되는 장기적인 측면의 모든 건강정보의 집합[28]으로 정의할 수 있다.

---

26) 보건의료기본법 제3조 제6호는 보건의료정보라 함은 보건의료와 관련한 지식 또는 부호, 숫자, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료를 말한다고 규정하고 있다. 또한 동법 제3조 제1호는 보건의료라 함은 국민의 건강을 보호, 증진하기 위하여 국가·지방자치단체·보건의료기관 또는 보건의료인 등이 행하는 모든 활동을 말한다고 규정하고 있다. 이와 같은 규정에 의하면 보건의료정보는 국민의 건강을 보호, 증진하기 위하여 국가·지방자치단체·보건의료기관 또는 보건의료인등이 행하는 모든 활동과 관련한 지식 또는 부호, 숫자, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료라고 정의할 수 있을 것이다.

27) 백윤철, "헌법상 환자의 의료정보에 대한 권리에 관한 연구", 헌법학연구 제11권 제3호, 2005.9. 343-344면

28)1. CPRI(Computer Based Patient Record)의 정보항목

첫째, Health 데이터로 Health과 관련된 문제들의 명세(진단, 증세, 진단연구와 판단의 결과 소견, 진찰과 상담기록 등 처방, 치료기록)과 Wellness 데이터(면역 이력, 위험 평가, 행동에 관한 데이터 그리고 환경적인 정보)가 있다.

둘째, 지식 원천으로부터 뽑아낸 정보로 전문가시스템과 의사결정지원 기능(개인들의 건강보호를 직접적으로 기여하는 치료 규칙, 보호 계획 그리고 임계경로), 그리고 환자 교육 데이터(약물치료 관리 설명서, 추천된 절차 지침서)가 있다.

셋째, 관리적인 데이터로 환자 기록 정보(인구통계학적, 공급자 확인, 돌보는 사람 확인, care에대한 데이터와 시간, "누가", "무엇을", "언제", "어디서" 데이터를 추출하였는지에 대한 데이터)와 재정적인 데이터(건강 보험과 사회보장 서비스)가 있다.

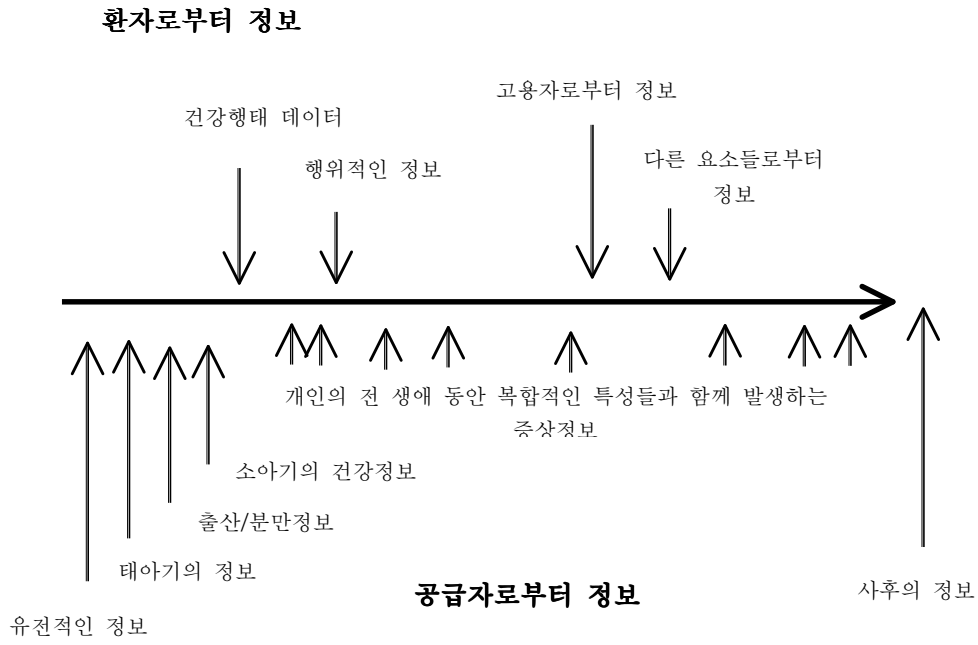

그림 1 의료 정보

2.2.1.2 의료정보의 특성

의료분야에 있어서 문제가 되는 개인정보는 의료의 본래적인 목적과의 관계상 환자인 개인의 질병에 관한 정보가 중심이 된다. 통상 의료정보란

넷째, 정보보안과 법적 측면의 데이터로 개인적인 지도(치료를 위한 동의, 사전 지도, 정보 양도에 대한 권한), 데이터의 접근기록과 보관인(수탁자) 정보가 있다.
2. ASTM(American Society for Testing Materials)의 정보항목
첫째, 행정적인 데이터로 인구통계학, 법적인 동의, 재정적인 정보, 공급자/개업가 정보가 있다.
둘째, 임상적인 데이터(문제/진단)로 문제 리스트 정보가 있다.
셋째, 임상적인 데이터(병력)으로 면역, 위험한 스트레스 노출, 건강 병력 정보가 있다.
넷째, 임상적인 데이터(평가/시험)로 평가, 환자 보고 데이터가 있다.
다섯째, 임상적인 데이터(보호/치료 계획)로 임상 처방 정보가 있다.
여섯째, 임상적인 데이터(서비스)로 진단 테스트, 약물투여, 사전예약 정보가 있다.
일곱째, 행정적인 데이터로 행정적인 데이터, 기질이 있다.
여덟째, 임상적인 데이터로 주된 병/진단, 임상 경로, 치료/절차가 있다.

의료제공의 필요성을 판단하고, 또는 의료 제공을 행하기 위하여 진료 등을 통해서 얻은 환자의 건강상태 등에 관한 정보를 말한다. 이것이 지면 등의 매체에 기록된 것이 의료기록이며, 의료종사자가 작성한 간호기록, 처방전, 검사기록, 엑스선 사진 등을 포함하고 있다. 그리고 의료 정보는, 의료종사자가 적절한 의료를 제공하기 위하여, 그 과정을 기록화하여, 자신의 의료업무의 적합한 관리를 통해서 적절한 의료의 제공에 투자하는 점에 주된 목적이 있다고 이해되어 왔으나, 동시에 사회보험, 소송, 교육, 연구 및 생명보험, 손해보험 등에서도 이용된다고 하는 특색을 가지고 있다. 의료정보의 보유주체는, 의료기관, 또는 의료종사자에 한정되지 않고 다양하다. 또 의료 기관만을 보아서도, 국공립병원 이외에 민간의료기관도 포함하고, 그 지위를 보아서도 국가공무원, 지방공무원, 민간으로 갈라져 있다고 하는 점에서 다양성을 지니고 있다. 의료정보는 개인정보성, 전문성, 공익성을 갖는다. 우선 의료정보는 개인정보이며, 이러한 개인정보는 의료행위를 통하여 얻어진 산물이기 때문에 전문성을 갖고, 이는 또한 공익성[29]을 갖게 된다. 이렇듯 의료정보는 개인정보성을 갖기 때문에 소극적 방어권으로서의 사생활의 비밀유지권의 보호대상이기도 하지만 현대사회에서 개인정보는 각종 영역의 공공정책의 결정과 집행에 필수적이라는 점 때문에 공익성을 가질 수밖에 없다. 특히 의료정보의 경우 특히 지금처럼 한 명의 의사가 환자에 대한 모든 진료를 행하는 것이 아니라 다수의 의사, 간호사, 의료기사들이 관여되는 집단적 의료행위의 경우에는 의료진들 사이의 의사소통을 위해서는 환자에 대한 보건의료정보의 공유가 필수적인 역할을 한다는 점, 또한 의료정보는 의학연구 및 보건정책의 수립 및 집행이나 건강보험 등 복지정책에 있어서도 중요한 역할을 하고 있다는 점에서 특히 그러하다. 따라서 의료정보가 가지는 개인정보성, 전문성, 공익성을 아우를 수

29) 공공기관이든 민간단체든 개인이 제공하여 관리되는 개인정보는 공적 성격을 인정하여야 한다.

있는 의료정보보호방안에 관한 연구는 유의미하다 하겠다.

2.2.1.3 의료정보의 분류

의료정보는 환자가 의사를 접견하기까지의 단계를 중심으로 처음 병원에 가서 작성하는 환자기초정보가 있으며, 환자의 증상 및 검사 결과와 같은 객관적인 사실에 관한 환자건강정보 및 이를 기초로 의사가 평가한 진단정보를 의미하는 전문의료정보가 있고, 이들 기록들이 데이터베이스화한 경우인 원무정보가 있다. 이러한 정보 중에 환자기초정보는 환자에 의해서 기록되는 문서이므로 적절한 방식으로 작성, 수정되어야 하며, 정당한 사유 없이 개인의 의료정보를 탐지하거나 유출, 변조해서는 안 된다. 그리고 환자건강정보나 진단정보는 개인정보통제권을 기초로 보호를 받으며, 따라서 공공의 이익 내지 공공의 필요에 의하여 열람하는 것이 가능한 자료이며, 원무정보는 의료법이 정하는 범위에서 보호를 받으며, 또한 의료기관과 보험자에게 허용된 정당한 목적 범위 내에서 사용되어야 한다[30].

이러한 분류는 앞서 살펴보았던 개인정보의 2가지 분류법과 결합하여 그 의미가 있다. 먼저 식별가능성에 따른 분류에 따를 경우, 환자기초정보와 원무정보가 제외된 전문의료정보는 익명정보가 되며 그 보호의 정도가 약화된다. 다만, 유전자 정보와 같은 경우는 제한이 필요할 것이다. 그리고 보호 정도에 따른 분류법에 따를 경우도 의료정보는 절대적 개인정보로서 가장 강력한 보호가 요청될 것이나 식별자가 삭제된 전문의료정보는 공공의 필요에 따라 활용이 가능해지는 상대적 개인정보로의 전환이 가능해 진다.

---

30) 백윤철, "헌법상 환자의 의료정보에 대한 권리에 관한 연구", 헌법학 연구 제11권 제3호 2005, 344면

2.2.2 의료정보의 보호

2.2.2.1 의료정보 보호의 의의

의료정보는 의사와 환자 사이에서 이루어져 생산된다. 이는 개인의 건강에 관한 사항으로서 사생활적 요소가 강하다. 기본적으로 개인의 사적 비밀에 속하게 되므로, 그 보호는 의사 등의 의료인에게 비밀 유지 의무가 법률상 부과됨으로써 이루어진다. 의료정보는 이 법률상 비밀유지 의무에 상응하는 국민의 비밀유지청구권이라는 법률상 권리의 보호 대상이 되는 법익이라 할 수 있다. 하지만 오늘날의 정보사회에서 보다 더 중요하게 인식되는 의료정보의 의미는 첫째 그것이 최고규범인 헌법상 권리인 개인정보통제권 즉 헌법상 권리의 규범영역으로서 보호되는 '개인정보'가 된다는 점, 둘째 의료정보의 공적 활용 내지 공동 활용에 관련한 공익성이 크다는 점 , 셋째 정보사회에 있어서 -특히 이 연구의 경우 보건의료정보화를 통해서 개인의료정보의 전송 및 공유가 용이해짐에 따라- 개인정보가 빠르고 광범위하게 침해될 가능성 또한 증가한다는 현실과 밀접한 관련성을 가진다는 점 등의 내용을 지니고 있다는 것이다.

2.2.2.2 의료정보와 프라이버시권

오늘날 프라이버시권의 개념이 전통적 프라이버시권에서 현대적 개인정보통제권으로 바뀌어 오고 있음의 주지의 사실이다. 그러나 의료분야에 있어서 현대적 개인정보통제권의 보호뿐만 아니라 전통적 프라이버시권의 보호도 중요하다. 이는 다음과 같은 이유에 의해서이다.

우선, 첫 번째는 오늘날의 의료가 의사 한사람에 의해서만 행해지는 것

이 아니게 되었다는 점이다. 예를 들어서, 병원에서는 의사의 지시를 받아, 간호사와 약사를 비롯한 여러 직종의 의료 종사자가 환자에게 의료행위를 가하고 있다. 또, 특히 전문적인 자격이 없는 사무직원과 위탁직원 등도 의료에 관여를 하게 되고 있다.

뿐만 아니라 몇몇 의료시설과 의료 관련 시설의 제휴로 인해 환자 한 사람에 대한 의료행위가 행해지는 경우[31]나 고령화 사회의 도래로 인한 보건・의료・복지의 제휴의 경우[32] 그들 시설 간에서 환자에 대한 정보를 교환하기 때문에 더 많은 사람들이 의료에 관여하게 된다.

이처럼 오늘날에는 환자의 치료에 의사 이외의 많은 직종이 관여하고 있으며, 이로 인해 환자의 개인정보를 아는 자가 증가하게 되었다. 따라서 필연적으로 개인정보로서 의료정보가 침해될 위험은 커지게 되는 것이다. 특히 기술한 바와 같이 법률 등에서 비밀유지의무가 부과되어 있지 않은 의료 관계 이외 직종의 의료에의 관여는 전통적 프라이버시권을 보호함에 있어서 중요한 문제를 일으키고 있다.

두 번째는 의사와 환자 이외의 제삼자, 즉 보험관계단체, 행정, 의학연구자 등의 의료에의 개입이다. 특히 오늘날과 같이 의료인에게만 환자정보에 대한 비밀유지의무를 부과하고 있는 의료법체계에서는 이처럼 제삼자의 의료로의 개입도 환자의 개인정보로서 의료정보를 보호하는데 있어서 중요한 문제이다.

세 번째는 정보기술과 통신기술의 도입이다. 의료 분야에도 기하급수적

---

31) 최근 의료 현장에 있어서는, 의료시설 상호간에 환자가 큰 병원으로 집중되고 있는 현실과 의료시설 간의 역할 분담이 불명확성으로 인해 의료자원의 활용에 낭비가 발생하고 의료분야 전체의 효율이 저하하고 있다는 등의 의료공급체계의 문제점이 지적되어, 이를 시정하기 위한 하나의 방책으로서 의료시설 상호의 제휴의 필요성이 지적되고 있다.

32) 어떤 환자가 의료의 손을 떠나 보건이나 복지 분야의 사람들에게 케어를 맡겨, 충실한 케어가 제공되도록 하고자 할 경우에는 의료시설간의 제휴와 마찬가지로 해당 환자의 의료에 관한 정보가 보건이나 복지에 종사하는 사람들에게 전달되게 되어, 이 사람들도 환자의 개인정보를 알게 될 수 있는 기회를 갖게 되는 것이다.

으로 증가하고 있는 정보를 효율적으로 관리하기 위하여 정보기술과 통신기술이 도입되고 있다. 그러나 의료정보보호에 관한 기준 및 교육이 미비한 상태에서 정보기술 및 통신기술의 도입은 어떤 의미에서는 환자의 개인정보로서 의료정보를 침해할 위험을 증대시키고 있다.

따라서 의료정보에 있어 전통적인 프라이버시권의 효과적인 보호를 위하여 의료인외에 의료정보취급자의 비밀유지의무에 대한 고찰 또한 중요한 의미를 지니게 된다.

2.2.2.3 의료정보와 개인정보통제권

보건의료정보화에 따른 의료정보의 전산화 및 집적은 의료정보의 내용 및 정보의 유용성과 공익성으로 말미암아 다른 어떠한 정보보다 강한 준공공재로서의 성격을 갖는다. 의료정보의 공유 및 활용으로 말미암아 발생하게 될 보건의료서비스 제공의 효율성 향상 및 의학의 발전 등 다양한 공공의 이익을 고려할 때 더욱 그러하다. 그러나 의료정보는 공익적 성격 뿐 아니라 궁극적으로 개인에 대한 정보이기 때문에 공동체의 이익 및 운영과 직접적으로 관련이 없는 정보일 경우 개인의 인격성의 보호라는 전통적 프라이버시권의 보호를 받아야 한다. 이에 대하여 개인정보통제권은 공적 성격과 사적 성격을 가지는 개인 정보로서 의료정보를 인정하는 이론적 근거를 제시한다. 즉, 의료정보는 법적 근거에 의하거나 자발적으로 제공되어 관리되는 경우, 사생활정보로서의 성격이 완화되고 오히려 공적 정보로서의 성격을 강하게 가지게 되지만, 완전히 공적 성격만을 가지는 것이 아니기 때문에 의료정보에 대한 불법적 침해에 대해서는 사생활 정보로서의 성격을 여전히 주장할 수 있다[33]. 따라서 독자적인 헌법적 기본권으로서의

33) 김종철, 앞의 논문, 37-38면

개인정보통제권은 의료정보의 공동 활용과 개인의료정보보호라는 시대적인 요청을 모두 포괄할 수 있는 이론적 토대가 된다.

2.3 소결

개인정보의 일종인 의료정보는 보건의료공급자가 환자에 대한 의료행위를 하면서 수집된 자료들과 이 자료들을 기초로 하여 연구·분석된 정보들을 포괄하는 것으로서 개인의 전 생애에 걸쳐서 환자와 보건의료공급자로부터 수집되는 장기적인 측면의 모든 건강정보의 집합들을 의미한다. 이러한 의료정보는 궁극적으로는 개인에 대한 정보이기 때문에 인간의 존엄성과 자유의 중요한 요소로서 인격적 성질을 가지고 있는 것이므로 보호의 이익이 있는 일정한 경우 프라이버시권으로서 헌법적 보호를 받아야 함은 주지의 사실이다. 그러나 특히 현대사회와 같이 정보화 사회가 되어 컴퓨터로 대량의 개인정보가 집적되고, 대량의 정보가 순식간에 송신되는 시대에 있어서 의료정보는 헌법상 국가로부터 사생활을 침해당하지 않을 소극적 프라이버시권 및 개인정보에 대하여 자기가 결정할 수 있는 적극적 프라이버시권으로 보호되는데 그치지 아니하고 개인정보성과 의료정보의 활용과 관련한 개인정보의 공익성을 아우르는 개인정보통제권에 의해 보호된다. 이러한 개인정보로서 의료정보통제권은 정보주체와 정보취급자에게 일정한 권리와 의무를 부과하게 되는데 그 권리·의무의 내용으로는 타인에게 알리고 싶지 않다고 생각하는 것이 정당한 일정한 사적인 의료정보에 관하여 개인정보의 수집 및 획득, 개인정보의 보유 및 이용, 개인정보의 열람 및 제공, 개인정보의 침해 각각의 단계에서 정보주체에 의한 통제권 보장을 요구함과 동시에 이러한 권리를 실효적으로 확보하기 위하여 개인정보의 열람청구권 및 정정청구권을 도출하며 나아가 정보취급자에게 정보수집의

목적이외에 사용하지 않거나 비밀유지 및 정보보안에 철저할 것을 요구한다. 다음은 개인정보통제권의 내용으로 도출해 낸 의료정보보호의 쟁점 사항이다.

<table>
<tr><td rowspan="2">분 류</td><td rowspan="2">의료정보주체의 권리</td><td colspan="2">의료정보 취급자의 의무</td></tr>
<tr><td>사생활 보호</td><td>안전 보호</td></tr>
<tr><td>정보 수집 및 취득 단계</td><td>수집 전 환자의 동의를 구하고 얻을 권리 관련</td><td rowspan="4">비밀유지 의무</td><td>관리적</td></tr>
<tr><td>정보 보유 및 이용 단계</td><td rowspan="2">의료정보접근권,
정정청구권,
개시기록의 고지권
및 제시권 관련</td><td rowspan="2">물리적</td></tr>
<tr><td>정보 열람 및 제공 단계</td></tr>
<tr><td>정보 침해 단계</td><td>손해배상청구권 및
이용 및 제공의 통제 권리
관련</td><td>기술적</td></tr>
</table>

표 1 개인정보통제권에 근거한 의료정보보호의 쟁점 사항

그러나 주지하다시피, 개인정보통제권에 의해 정보주체 및 정보취급자에게 일정한 권리·의무를 부과함으로써 담보되는 개인정보로서 의료정보는 공공성 및 공익성 이라는 성격상 절대적으로 보호되는 것이 아니다. 즉 공동체 운영과 직접적으로 관련이 없는 정보는 개인의 인격성의 보호라는 전통적 프라이버시의 보호 차원에서 보호되어야 하지만 공동체의 공익 및 기타 사회적 필요에 의한 적법한 정보의 이용 및 공유도 담보하는 것이기에, 개인정보통제권에 의해 보장되는 의료정보를 어느 정도로 보호할 것인

가에 대한 구체적인 검토가 요구된다. 앞서 살펴보았듯 의료정보는 환자기초정보, 환자건강정보와 진단정보, 원무정보로 나누어진다. 이러한 세부적인 분류는 서로 통합 및 분리가 가능하며 이에 따라 식별가능성 및 민감도가 다른 정보로 구분되어질 수 있으므로 어떤 의료정보를 어느 정도로 보호할 것인가 하는 실천적 문제에 대한 해법의 하나로서 제시될 수 있을 것이다.

개인정보는 그 성격상 일단 침해되어 버리면 회복하는 것이 곤란하고, 오늘날과 같은 정보화 사회에서는 그 침해의 가능성이 매우 크며, 특히 의료정보는 매우 민감한 정보이기 때문에 더욱 강하게 보호되어야 할 필요가 있다. 그러므로 헌법상 보호되는 개인정보통제권을 보장하기 위해서는 사전에 의료정보가 침해되지 않도록 하는 보호조치를 취하는 것이 법·정책적으로 중요하다. 그리하여 요구되는 것이 의료정보보호제도인 것이다.

제3장 외국의 의료정보보호제도

3.1 외국의 개인정보보호법제

정보화는 이제 전 세계적인 흐름이 되었고 이러한 상황에서 개인정보를 보호하기 위하여 각 국은 그들의 사정에 맞는 법제도를 개발하여 시행하는 등 다각적인 노력을 펼치고 있다. IT 강국으로 떠오르고 있는 우리나라의 경우 헌법상 기본권인 개인정보통제권의 실현과 관련한 개인정보보호 현황은 다른 나라와 비교하여 상당히 앞서가는 면도 있고 뒤처진 면도 있다. 특히 컴퓨터를 이용하여 전 세계가 하나의 정보통신망을 구축하게 된 현대에 이르러 개인정보 보호의 문제는 국내뿐 아니라 국제적인 문제라 할 수 있을 것이므로, 다른 나라 제도를 검토하는 것은 중요한 과제라 할 것이다. 따라서 먼저 국외의 개인정보 보호제도를 살펴보고, 이를 통해 개인정보로서 의료정보의 구체적인 보호방안을 마련하는데 있어 적용해야할 원칙 및 기준을 도출해 내는 것은 의미가 있을 것이다.[34)]

3.1.1 OECD이사회의 가이드 라인

국제기관에 의한 개인정보보호의 대응방법으로 지침적인 역할을 하고 있는 것이 경제협력개발기구가 1980년 9월 23일 채택한 '프라이버시 보호와 개인데이터의 국제유통에 관한 가이드라인에 대한 이사회권고'[35)] 이다.

---

34) 백윤철, "인터넷과 개인정보보호", 신영사, 2002 참조

35) OECD가이드라인과 같은 국제적인 개인정보보호를 위한 가이드라인이 요구되는 이유는 컴퓨터에 의해 대량의 개인정보가 처리됨에 따라 이들의 자유로운 유통을 확보하면서도 적절한 보호가 필요하게 되었는데, 이를 위해 각국의 법제도의 통일성이 필요하게 되었

이 OECD권고는 개인정보의 보호를 위하여 8개의 원칙을 제시하였다. 이를 의료정보에 관련하여 살펴보면 다음과 같다.

원 칙	내용	의료정보보호 적용
수집제한의 원칙	개인데이터의 수집에는 제한을 두어야 하며, 어떠한 개인정보도 적법하고 공정한 수단에 의해 수집되어야 한다	유전자 정보나 가족의 질병 내력
정보정확성의 원칙	개인정보는 사용목적과 범위가 부합되어야 하며, 정확하고 완전하며 갱신되어야 한다	보험청구의 허위
목적명확화의 원칙	개인정보를 수집할 때에는 목적이 명확해야 하고, 이를 이용할 경우에도 최초의 목적과 모순되지 않아야 한다	연구목적과 건강권 내지 보건권을 위해 목적을 명확히 해야 한다
이용제한의 원칙	개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화된 목적 이외의 용도로 공개되거나 이용되어서는 안된다	진료, 보험 이외의 이용에 대하여 제한 및 허용기준이 필요
안전보호의 원칙	수집 및 보존하고 있는 개인정보의 분실, 불법적인 접근, 파괴, 정보수정 및 공개와 같은 위험에 대비하여 합리적인 안전보호장치를 마련해야 한다	개인정보의 유출을 방지하기 위한 방호시스템을 확보해야 한다

기 때문이다. 그리하여 개인정보의 보호와 자유로운 상거래가 균형을 이루도록 OECD 각국이 만족할 만한 개인정보 보호의 수준을 이사회 권고로서 정리하였고, 각국은 이 권고에 따라 자국의 제도를 정비한다는 합의를 하였는데, 이것이 'OECD권고'이다.

개인참가의 원칙	개인정보를 제공한 개인은 자신과 관련된 정보의 존재확인, 열람요구, 이의제기 및 정정・삭제・보완 청구권을 갖는다	의료인의 역할과 판단에 대한 근거 요구와 환자의 동의가 있어야 의료정보를 이용할 수 있다
공개의 원칙	개인정보에 관한 개발, 운용 및 정책에 있어 일반적인 공개의 원칙이 적용되어야 한다	의료정보의 흐름에 대한 공개
책임의 원칙	개인정보를 관리하는 자는 이에 대한 책임을 져야 한다	의료정보 주체에 대한 책임

표 2 OECD권고에 나타난 개인정보보호를 위한 8개의 원칙

개인정보 보호와 관련된 법과 제도들은 국내・외를 막론하고 이와 같은 OECD가 제정한 8가지 원칙에 기초하고 있다.

3.1.2 유럽평의회의 개인데이터보호조약

OECD 가이드라인이 개인정보의 보호를 위한 지침을 규정하고 있음에도 불구하고 정보통신기술의 발달로 인해 정보의 보호 필요성이 더욱 절실해짐에 따라 자동 처리되는 개인정보를 더욱 보호하기 위한 목적으로 유럽에서 '개인데이터의 자동처리에 관한 개인의 보호에 관한 조약'[36]이 체결되었다.

36) 이 조약은 OECD 가이드라인이 채택된 다음 해에 유럽평의회에서 인준되고 1985년에 발효되었다. 이 조약은 기본적으로는 OECD이사회 권고와 거의 같은 원칙에 기초한 것이지만, 단순한 권고가 아니라 조약이기 때문에 유럽에서는 OECD가이드라인보다도 가맹국에 대한 구속력이 강하다. 그러나 OECD가이드라인과는 달리 유럽 이외의 지역에서는 적용되지 않는다. 백윤철, "우리나라에서 의료정보와 개인정보보호", 헌법학 연구 제11권 제3호, 2005, 402-403면

유럽평의회 조약은 ①데이터의 취득 및 처리의 공정함, ②합법적인 목적에서의 이용과 축적, ③개인정보의 처리목적이 적절할 것과 목적 이외로 정보처리하지 않을 것, ④정보의 정확성 및 갱신, ⑤필요한 기간을 넘긴 데이터 축적의 금지 등에 대해서 규정[37]하고 있으며 가맹국에 대해서 이 조약에 적합한 법률의 제정을 요구하는 내용으로 되어 있다. 본 조약에서도 의료정보에 대한 취득 및 처리의 공정함, 합목적인 이용, 유출에 대한 책임 등을 규정하고 있다고 해석된다.

3.1.3 EU의 개인데이터 보호지침

'개인데이터 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 1995년 10월 24일의 유럽의회 및 이사회의 95/46/EC지침'[38]은 자동처리 및 수동 처리된 개인데이터의 처리에 적용된다.

EU 지침[39]에 있어서는 개인정보보호에 대해서 다양한 규정을 두고 있으나, 특히 제25조는 "가맹국은 처리과정에 있는 개인 데이터 또는 이전 후 처리하는 것을 목적으로 하는 개인데이터의 제3국에의 이전은 이 지침 외의 규정에 따라서 채택된 그 나라의 규정의 준수를 위반하지 않고, 해당 제3국이 충분한 수준의 보호를 확보하고 있는 경우에 한하여 행하는 것이 가능하다고 하는 것을 규정해야만 한다"고 규정하고 있는데, 그 취지는

37) 백윤철, "우리나라에서 의료정보와 개인정보보호" 앞의 논문, 402-403면

38) 유럽위원회(European Commission)는 1980년의 OECD가이드라인 및 1981년의 유럽평의회 조약이 개인정보보호를 둘러싼 그 후의 상황에 충분히 대응하고 있지 못하며, 가맹국에서 제정된 데이터보호를 목적으로 하는 다양한 법률이 정한 보호 수준이 일정치 않다고 판단하였다. 이러한 배경에서 1990년 9월에 국내법을 조정함으로써 개인 데이터의 자유로운 유통을 확보하는 것을 목적으로 하는 지침의 기초안을 제의하였고, 5년 후에 채택되었다. 백윤철, 앞의 논문, 403-406면

39) Directive 95/461EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

EU가맹국에 대해서 EU 지침에 적합하도록 현행 국내법의 개정과 새로운 법률의 제정을 요구하고, 개인정보의 보호에 관하여 충분한 수준의 보호조치를 가지고 있지 않은 나라에 개인 데이터의 이전을 금지하는 것이 가능하다는 취지의 규정을 국내법으로 만들 것을 요구하는 것이다[40].

또한 개인데이터의 이전이 허용될지 여부에 대해서 검토가 이루어질 때에는 ①데이터의 성질, ②실행되는 데이터 처리의 목적 및 기간, ③데이터의 생성국 및 최종 이전국, ④제3국에 있어서 효력을 가지고 있는 법률(포괄법 및 개별분야별법 등), ⑤제3국에 있어서 적용되는 직업규정 및 안전기준 등이 고려의 대상[41]으로 되어 있다. 이런 사항에 대해서 검토한 결과 개인정보의 보호에 대해서 '충분한 수준의 보호'를 확보하고 있지 않다고 생각되는 나라에 대해서는 데이터의 이전을 금할 수 있게 되었다. 이러한 기준은 의료정보의 이용 및 공유에 있어 그 적용이 가능할 것으로 판단된다. 구체적인 사항은 아래와 같다.

EU 지침 고려대상	의료정보 제3자 이전
데이터의 성질	의료정보의 민감도 및 식별가능성
실행되는 데이터 처리의 목적 및 기간	의료정보이용의 목적 및 기간
데이터의 생성국 및 최종 이전국	의료정보의 최종 목적지
제3국에 있어서 효력을 가지고 있는 법률	제3자의 의료정보보호 방침
제3국에 있어서 적용되는 직업규정 및 안전기준	제3자의 의료정보보호 안전조치

표 3 개인데이터의 제3국에의 이전 허용시 고려사항

또한 특정의 조건에 해당하는 경우에는 데이터의 이전을 허용하도록

40) 개인데이터의 제3국 이전, 제3자정보이전
41) 백윤철, 앞의 논문, 405-406면

법률로 정하는 것이 가능하도록 되어 있다. 그 조건으로는 ① 데이터 주체로부터 명시적인 동의를 얻은 경우, ② 데이터 이전이 관리자와 데이터 주체 사이에 맺어진 계약에 기초하여 이전하거나 또는 정보주체가 요구하는 전계약에 기초하고 있는 경우, ③데이터의 이전이 관리자와 데이터주체의 이익의 범위 내에 있는 제3자 사이에서 맺어진 계약에 기초한 경우 ④데이터의 이전이 중요한 공공이익에 기초하는 경우 또는 법적인 요구에 관한 것인 경우, ⑤데이터의 이전이 데이터 주체의 생존에 불가결한 이익의 보호를 위한 경우, ⑥데이터의 이전이 정당한 이익을 가지는 인물이 참조하는 목적으로 개시된 경우 등이 정해져 있다.

데이터 이전이 허용되는 예외적인 경우에 대한 제시는 공익성과 개인성을 가지는 의료정보의 공유 및 활용에 있어, 개인정보통제권이 적법한 범위 내에서 제한될 수 있는 합리적인 기준을 제시할 수 있을 것으로 판단된다.

3.2 외국의 의료정보보호 법제

3.2.1 미국

3.2.1.1 HIPAA 규정

미국은 의료보험과 관련하여 보건의료정보의 교환과 처리에 있어 책임과 보호에 대해 규정하고 있는 HIPAA(Health Insurance Portability and Accountability Act)를 국회에서 1996년 8월에 법률화하였다. 그러나 주를 초월하여 미국 전역 어디를 가더라도 의료보험의 이전이 자연스럽게 이루어지기 위해서는 미국 전역에 있어서의 의료정보의 표준화가 필요하였으며, 그와 함께 안전보호, 프라이버시보호를 동반할 필요가 있었다. 이를 위하여 5개의 title로 구성된 HIPAA법 중 TitleⅡ(의료비사기나 의료비남용의 방지·의료사무의 간소화·의료과오소송개혁) Subtitle F(의료사무의 단순화) 이하에서 미국전역의 의료기관에서 의료정보를 보호하기 위한 규칙제정을 명문으로 규정하였고, 이를 기반으로 미국의 의료정보에 관한 프라이버시 규칙[42]이 2003년 4월 14일부터 시행[43]되었다. 이 법률에 의해 비로소 미국의 환자들은 자신의 의료정보에 관하여 전국적으로 통일된 보호 규칙을 적용받게 되었다. HIPAA프라이버시규칙의 특징[44]은 다음과 같다.

① 의료정보취급의 투명성을 보장하기 위하여 각 의료기관은 각 환자에게 의료정보취급방침을 통지하여야 한다.

② 환자는 의료정보에 관한 3가지의 권리 개시청구권[45], 정정청구

42) The standards for Privacy of Individually Identifiable Health Information
43) Public Law 104-191 (제104의회에서 제정된 109번째 법률)
44) 백윤철, "미국의 HIPAA법에 관한 연구", 인터넷법률 통권 제31호 2005.9, 55-56면

권[46], 설명보고[47]를 받을 권리를 가진다.

③ 의료기관이 환자의 동의없이 환자정보를 이용할 수 있는 경우는 치료, 지불, 의료업무관리(TPO : **treat**men**t**, pa**y**men**t**, he**a**lth **care** oper**at**ion)에 사용되는 경우로 한정하였다.

④ 치료, 지불, 의료업무관리 이외의 경우[48] 정보취급방침에 대하여 원칙과 예외를 구분하여 상세히 규정하고 있다.

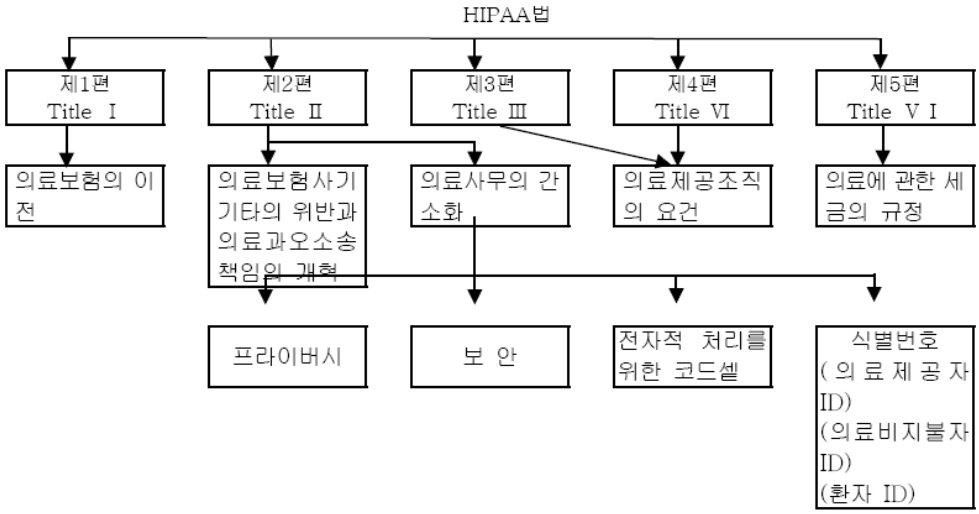

그림 2 HIPAA법의 구조

45) 자신의 의료기록을 검사, 열람하고 복사를 청구할 권리
46) 열람한 의료기록의 내용에 잘못이 있으면 정정을 청구할 권리
47) 과거 6년에 걸쳐 자신의 의료기록이 이용된 상황에 관한 설명보고를 받을 권리
48) 환자명부 등재가능여부, 가족에 대한 개시, 연구이용, 마케팅, 공중위생 및 법집행 등위한 개시의 경우 등이 있다.

3.2.1.2 의료정보의 소유권

미국의 경우 의무기록의 소유권은 그 정보를 작성한 의료기관에 있는 것으로 본다[49]. 따라서 의료기관은 의무기록의 물적 형태를 소유할 권리를 가진다. 그러나 그 매체가 포함하고 있는 환자정보의 내용에는 적용되지 않고, 환자정보의 내용의 소유는 환자에 속한 것으로 한다. 그리하여 일부 주는 환자 정보는 법원의 명령에 의하지 않고는 의료기관 밖으로 내어갈 수 없도록 하였다. 의료기관에게 물적 형태의 개인의료정보 소유권을 인정하는 근거는 의무기록이 환자진료의 지속성 확보를 위한 주요 수단으로 법적인 자료로서 의료의 거래에 있어서 의료인과 환자를 동시에 보호한다는 것이다. 의무기록에 기록된 자료는 의료종사자들의 진료의 질 보장, 평가, 향상을 위한 연구에 필요한 정보를 제공하는 것으로 진료수행에 대한 증거가 되며, 보험청구 내용을 증명하기 위한 기본 자료로서 의료기관이 보유하여야 하는 것으로 판단하기 때문이다[50].

3.2.1.3 의료정보의 열람

미국의 현행법이나 판례에 의하여 대부분의 주에서 환자의 알 권리가 인정되고 있다. 정보공개의 이유는 의무기록에 기록된 환자 자신의 정보를 알고, 이 정보가 제3자에게 주어졌을 때 자신에게 어떤 영향을 줄 것인가에 대한 알 권리를 보호한다는 것이다. 이러한 정보의 공개는 환자의 의사에 대한 신뢰성 확보에 기여하며, 환자 자신의 건강상태에 대해 정확히 알게 됨으로써 건강회복에 긍정적인 영향을 줄 수 있다. 환자가 보건의료기

49) 윤경일, "정보화시대의 환자진료정보 보호에 관한 법·제도적 고찰", 병원경영학회지 제8권 제2호, 116면
50) 김곤희, 앞의 논문, 46-47면

관의 서비스에 비용을 지불하였으므로 환자가 자신의 의무기록에 접근함이 타당하다[51]는 접근이다.

3.2.1.4 정보의 제3자 공개

HIPAA의 경우, 진료정보를 진료, 의료보험 청구 등을 제외한 목적으로 공개하거나 사용 시에는 환자의 동의서를 구해야 하며, 목적을 달성하기 위한 최소의 정보만을 사용하여야 한다. 환자개인을 식별할 수 있는 변수가 제외된 정보는 자유로이 사용되고 공개될 수 있다.

3.2.2 일본

일본에서는 2003년「개인정보의 보호에 관한 법률」이 제정되어 2005년 4월부터 전면적으로 시행되고 있으며, 개인정보보호법의 전면시행과 관련하여 의학연구에 있어서의 개인정보의 취급에 관해서는 특별히 적정한 취급을 확보하는 분야로서 관계 각성의 심의회·위원회에서 검토되어, 2004년 12월에「의료·개호관계사업자에 있어서의 개인정보의 적절한 취급을 위한 가이드라인」이 책정·공표되었다. 이러한 개정지침은 2005년 4월부터 적용되고 있다.

그동안 일본에서 의료정보를 보호하기 위한 형사적인 포괄적 규제는 의사와 의료기관의 비밀누설에 따른 처벌조항[52]에 의해 이루어져 왔다. 또한 정보의 부당이용으로 인한 피해에 대한 구제는 민사법상 계약책임(진료계약 위반으로 인한 채무불이행책임) 또는 불법행위책임으로 추궁할 수 있

51) 김곤희, 앞의 논문, 46-47면
52) 일본형법 제134조, 일본의료법 제72조 등

다. 그러나 의료정보의 특수성과 보호의 중요성을 인식하여 특별법의 제정이 필요하다는 주장에 의해 2003년 5월에 제정되어 2005년 4월부터 시행된 개인정보보호법을 비롯한 5개 법률[53]이 의료정보보호에 중요한 역할을 하게 되었다고 볼 수 있다[54].

특히 이 법은 개인정보취급사업자에게 개인정보의 불법유출에 대한 무거운 책임을 지우고 있다. 즉 개인정보가 유출된 원인이 의료기관의 내부직원의 조작실수인지, 파견 직원의 부정사용목적에 의한 것인지를 묻지 않고, 최고 경영자가 과실이 없다는 것을 입증해야 한다. 정보누설의 원인을 명확히 알 수 없거나 복합적인 원인에 의한 경우가 많기 때문에 무과실 책임을 지게 되는 결과를 가져온다. 개인 의료정보취급사업자가 의무규정에 위반하여 개인의 권리나 이익보호를 위해 필요한 때에는 주무장관은 그 시정을 권고할 수 있고, 권고에 따르지 않는 경우에는 시정명령을 내릴 수 있다[55].

3.2.3 프랑스

의사의 직업상의 비밀 준수의 원칙은 환자의 권리와 보건시스템의 질에 관한 2002년 3월 4일 법률에 의하여 공중보건법전 제L 1110-4조에 선언되어 있다[56]. 비밀원칙을 지키지 않으면 형법전에 의하여 처벌받는다. 형법전 제226-13조는 "직무상 또는 일시적으로 상황이나 직업상 그에게 기탁된

53) 개인정보보호 관련 5개 법률은 「개인정보보호에관한법률(個人情報の保護に關する法律)」, 「행정기관이보유하는개인정보보호에관한법률(行政機關の保有する個人情報の保護に關する法律)」, 「독립행정법인등이보유하는개인정보보호에관한법률(獨立行政法人等の保有する個人情報の保護に關する法律)」, 「정보공개·개인정보보호심사회설치법(情報公開‧個人情報保護審査會設置法)」, 「행정기관이보유하는개인정보보호에관한법률등의시행에따른관계법률의정비등에관한법률(行政機關の保有する個人情報の保護に關する法律等の施行に伴う關係法律の整備等に關する法律)」등이 있다.

54) 연기영, "일본의 의료정보와 정보보호", 중아법학 제7집 제4호, 2005 참조

55) 일본개인정보보호법 제35조, 제48조 등

56) 사생활의 비밀은 의료서비스 제공 중에 지켜진다(공중보건법전 제L 1110-4조).

자의 비밀에 속하는 정보를 누설한 자는 1년간 금고 및 15000 유로의 벌금에 처한다."고 규정하고 있다.

2002년 3월 4일 법률은 첫째 1995년의 의료직무 법전의 내용을 보충, 강화, 확충하고, 명확히 하고 있으며, 둘째 비밀의 원칙을 이용자의 권리로 설정하는 한편, 직업상의 의무로 선언하고 있다.[57] 비밀의 의무의 법리적 근거에 관하여는 공공질서에 관한 절대적 이론(Thèe **abs**o**lutist**e d'**ordr**e p**ublic**)과 사익에 관한 상대적 이론(Thèe **relativist**e del'int**é**ê p**r**ivé)이 대립하였으나, 현실적인 해결책은 의사와 환자의 관계 및 의사와 제3자의 관계로 파악하고 있다.[58] 다른 한편, 이 원칙에 대한 몇몇 예외사항이 법률에 규정되어 있다. 물론 환자 자신이 의료정보열람을 신청한 경우나 의료 비밀의 공개를 요청한 경우는 예외로 한다.

환자의 권리와 보건시스템의 질에 관한 2002년 3월4일 법률에 의하여 공중보건법전 제L 1110-4조는 그러한 정보를 취득하거나 취득하려고 기도한 경우에도 1년간 금고 및 15000 유로의 벌금에 처한다.

다만 환자의 권리와 보건시스템의 질에 관한 2002년 3월 4일 법률에 의한 공중보건법전 제L1110-4조와 형법전 제226-14조는 법률이 부과하거나 허용하는 경우에는 비밀원칙이 적용되지 않는다고 규정하고 있다. 형법전 제226-14조는 의무적 또는 임의적인 비밀정보의 공개 케이스를 의무적 공개사항과 임의적 공개사항으로 나누어 규정한다. 의무적 공개사항으로는 공중보건 보호, 호적사무[59], 의료사고, 에이즈, 산재사고, 직업병, 유아에 대한 예방접종, 시민생활에 보호가 필요한 정신질환의 경우와 같이 환자의 이익보호 및 질서유지, 의료예산통제를 위한 경우가 있다. 임의적 공개사항

57) P. **Ab**adie **et** 8,op.**cit**. p.55.
58) G**é**ard M**é**e**teau**, Cou**rs** de d**roit** m**éical**, Le**s** Etudes Hospit**alièes**, 2003. p.249-274.
59) 민법전 제56조는 출산에 참석한 의사, 조산원, 공무원 기타 인원은 출생신고를 의무적으로 하도록 규정

으로는 연구나 평가, 분석 및 예방과 마약퇴치를 위한 경우와 같은 공중보건 보호를 위하거나 환자가 대리인을 지정한 경우 및 성범죄의 희생자나 미성년자 보호를 위한 경우[60] 등이 있다.

3.3 소결

병력 등과 같이 그 자체로서 내밀한 영역을 드러내는 민감한 개인정보인 경우에는 그 수집 내지 보유만으로도 인격 침해의 가능성이 크기 때문에 그 처리의 상황과 무관하게 특별히 강화된 보호를 필요로 한다. 특히 보건의료정보화는 정보가 짧은 시간 내에 대량으로 광범위한 상호 전달이 가능해 지기 때문에 이에 대한 적절한 보안대책과 조치가 없을 경우, 환자 사생활 침해의 개연성이 증가되는 동시에 대량의 환자정보에 대한 접근이 용이해지기 때문에 환자 개인 정보의 대량노출 가능성 또한 높아진다. 이로 인하여 환자와 의료서비스 제공자간의 상호작용에 악영향을 미칠 수 있다. 각국 및 국제기구의 개인정보 및 의료정보보호 법제·지침은 일찍이 의료정보의 특수성과 공익성을 파악하고 현실적으로 의료서비스의 질적 향상 및 효율성 향상을 위한 의료정보화에 있어 환자의 의료정보보호를 위하여 물리적인 보안뿐 아니라, 먼저 법·제도적으로 철저한 보호 및 보안체계를 마련하여 상호간의 신뢰를 형성하고 원활한 상호작용을 도모하고 있음을 살펴보았다.

특히 개인정보보호에 관한 일반원칙으로 국제적으로 인정받고 있는 OECD권고에 나타난 개인정보보호를 위한 8개의 원칙은 2장에서 살펴보았던 개인정보통제권의 제한원칙인 비례원칙의 파생원칙으로서, 의료정보화를 통한 의료서비스의 효율성 추구와 동시에 의료정보의 수집과 사용 과정

60) 15세 미만의 아동에 대한 성범죄는 사법당국이나 행정관청에 통지할 수 있다.

에서의 자기정보결정권에 근거한 의료정보의 보호를 모두 추구해 나가는 바람직한 의료정보 보호의 대원칙으로 이해될 수 있을 것이다.

이들 원칙을 의료정보보호에 적용하여 보면, 먼저 어떠한 개인정보도 적법하고 공정한 수단에 의해 수집되어야 한다는 수집제한의 원칙은 의료정보의 수집에 있어 환자의 알권리를 충족시키는 한편, 개인정보자기결정권에 근거하여 의료정보수집에 있어 동의를 요구하게 된다. 특히, 의료정보 중에서도 유전자 정보나 가족의 질병 내력 등의 수집에 있어 그 적용이 유의미하다.

둘째, 개인정보는 사용목적과 범위가 부합되어야 하며, 정확하고 완전하며 갱신되어야 한다는 정보정확성의 원칙은 정보에 대한 접근권 및 정정청구권을 전제하여야 하며 특히, 보험청구 및 취업 등 경제적인 관계와 맞물리는 경우 중요성이 크다. 수집된 개인정보가 내용에 있어 오류가 있거나 최근의 사정을 반영하고 있지 못할 경우 정보주체로서는 사회적, 경제적으로 다양한 피해를 입을 수 있기 때문이다.

셋째, 개인정보를 수집할 때에는 목적이 명확해야 하고, 이를 이용할 경우에도 최초의 목적과 모순되지 않아야 한다는 목적명확화의 원칙은 환자의 의료정보 수집 시 목적을 명확히 해야 하며, 이용 시에도 환자의 동의 및 연구목적과 건강권 내지 보건권 등 공익을 위해 목적을 명확히 해야 한다는 것을 요구한다. 한편 목적이 달성되었거나 그 목적을 달성하는데 더 이상 도움이 안 되는 경우에는 그 개인정보는 파기되어야 한다[61)62)].

넷째, 개인정보는 정보주체의 동의가 있는 경우나 법률의 규정에 의한 경우를 제외하고는 명확화 된 목적 이외의 용도로 공개되거나 이용되어서는 안 된다는 이용제한의 원칙은 기본적으로 진료, 보험의 경우 제한이 비

61) 영국 데이터보호법 제5원칙 참조

62) 이와 관련하여 문제되는 것이 바로 국민건강보험공단이나 심평원에 이용 목적이 달성되었음에도 불구하고 법률 상의 근거 없이 축적되어 있는 보험관련데이터이다.

교적 완화되지만 그 이외의 이용에 대하여 제한 및 허용기준이 필요함을 의미한다.

다섯째 안전보호의 원칙은 의료정보취급자에게 합리적인 안전보호 장치를 마련해야 한다는 의무를 부과한다. 필요한 목적을 위하여 수집된 개인정보가 아무렇게나 방치되거나 제3자에 의해 함부로 접근할 수 있도록 허술하게 관리될 경우 개인의 기본권은 무방비 상태에 있게 되는 것이다. 따라서 개인정보의 분식 또는 불법적인 접근, 파괴, 사용, 수정, 개시 등의 위험에 대비하여 합리적인 안전조치를 위하여야 한다.

여섯째, 개인정보를 제공한 개인은 자신과 관련된 정보의 존재확인, 열람요구, 이의제기 및 정정·삭제·보완 청구권을 갖는다는 개인 참가의 원칙은 개인정보자기결정권과 결합하여 궁극적으로 의료정보의 목적 내 이용에 대한 감시권도 포함하게 된다.

일곱째, 개인정보에 관한 개발, 운용 및 정책에 있어 일반적인 공개의 원칙이 적용되어야 한다는 공개의 원칙은 의료정보의 흐름에 대한 공개를 통해 환자의 알권리 및 개인정보자기결정권을 보장한다. 이는 어떠한 정보를 보유하고 있는지 공개하도록 함으로써 개인정보의 이용 및 처리에 대한 검증과 감시를 가능하게 하고 정보주체의 의료정보통제권의 행사를 용이하게 하기 위한 것이라 할 것이다.

마지막으로 개인정보를 관리하는 자는 이에 대한 책임을 져야 한다는 책임의 원칙을 통해 의료정보의 침해 시 의료정보 주체에 대한 책임을 강화함으로써 사전에 의료정보의 침해를 방지하는 효과를 줄 수 있을 것이다.

OECD권고에 나타난 개인정보보호를 위한 8개의 원칙이 주로 개인정보의 자기결정권에 근거한 사생활의 보호에 중점을 두는 기준으로 적용이 가능한 반면, 의료정보의 공적 목적에의 이용을 가능하게 하는 기준으로 적

용 가능한 원칙이 바로 '개인데이터 처리에 관한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 1995년 10월 24일의 유럽의회 및 이사회의 95/46/EC지침' 상에 제시된 개인데이터의 이전이 허용될지 여부에 대해서 검토할 경우 고려할 사항 및 제3국으로의 데이터의 이전이 허용되는 예외적인 경우이다. 의료정보의 제3자 이전 및 이용에 있어서도 EU지침을 활용하여 정보주체의 동의가 있을 경우에만 그 이전 및 이용을 인정하는 것을 원칙으로 하되, 의료정보의 이용이 중요한 공공이익 및 법적인 요구에 관한 것인 경우나 정보주체의 생존에 불가결한 이익 보호를 위한 것인 경우에는 예외적으로 그 이용을 허용하는 것으로 응용할 수 있을 것이다. 뿐만 아니라 제3자에게로 의료정보가 제공 및 이용될 경우에는 의료정보의 민감도 및 식별가능성, 의료정보이용의 목적 및 기간, 의료정보의 최종 목적지, 제3자의 의료정보보호 방침, 제3자의 의료정보보호 안전조치 등에 대한 검토가 이루어져야 할 것이다.

의료정보의 공유 및 활용을 통해 의료서비스의 질과 효율성을 향상시키는 한편 민감할 수밖에 없는 개인의 사생활을 동시에 보호하려고 하는, 상반되는 이익을 동시에 충족시키기 위해서는 일관되고 포괄적인 정보보호의 전제가 되는 기준 및 원칙이 필요하다. 그런 의미에서 OECD권고에 나타난 개인정보보호를 위한 8개의 원칙 및 EU지침 상의 기준은 헌법상 보장되는 개인정보통제권에서 도출되는 합리적인 의료정보보호의 근거가 될 것이다.

제4장 한국의 의료정보보호

4.1 한국의 의료정보보호 법제

현재 우리나라 법체계에서는 개인정보로서 의료정보를 보호하기 위하여 개별적인 입법을 하기 보다는 헌법, 형법, 정보통신관련법 및 의료관련 법률 등을 통하여 규율하고 있는 실정이다.

4.1.1 헌법

헌법 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다.”라고 규정하고 있으며 헌법 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.”라고 규정하여 개인의 사생활의 비밀을 보호[63]하고 있다.

4.1.2 형법

형법 제316조는 비밀침해행위를 처벌하도록 규정하고 있으며, 형법 제317조는 의사, 한의사, 치과의사, 약제사, 약종상, 조산사 등이 업무처리 중 지득한 타인의 비밀을 누설한 때에는 형법적 처벌[64]을 하도록 하고 있다.

---

63) 남효순, 앞의 책, 62-67면, 허영, “헌법이론과 헌법” 앞의 책, 502-506면
64) 이재상, “형법각론”, 박영사, 2006, 223-227면

4.1.3 정보통신 관련 법령

정보통신망이용촉진및정보보호등에관한법률 제21조 (전자문서 등의 공개제한) 및 제49조 (비밀 등의 보호), 전자서명법 제24조 (개인정보의 보호), 공공기관의개인정보보호에관한법률 제13조 (처리정보의 열람제한) 또한 개인정보보호의 근거가 된다. 공공기관의개인정보보호에관한법률 제4조, 제10조에는 국가행정 기관, 지방 자치 단체, 기타 공공단체 중 대통령령이 정하는 기관에서 개인 정보를 전산입력, 편집, 검색 등의 작업을 할 경우에 사상, 신조 등 개인의 기본적 인권을 현저히 침해할 우려가 있는 사항은 수집 할 수 없도록 규정하고 있고 이러한 정보를 이용하거나 다른 기관에 제공하는 것을 금하고 있다. 이 법의 제정은 정보화 사회에서 개인 정보의 보호가 중요한 쟁점으로 등장하였음을 단적으로 드러내는 것으로서 그 적용대상을 공공기관에 한정하고 있다는 한계점은 가지나, 개인정보의 보호를 위한 독자적인 최초의 법률이라는 점에 그 의의가 있다.

공공기관의개인정보보호에관한법률은 그 보호대상을 “공공기관의 컴퓨터에 의하여 처리되는 개인정보”로 규정하고 있는바, 공공기관의 컴퓨터에 저장되어 있는 개인의료정보는 동법 제10조, 제11조, 제22조 등에 의하여 보호받을 수 있다. 개인정보에 대해서 그 안정성을 확보하기 위하여 공공기관의 장은 개인정보를 처리함에 있어서 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 않도록 안전성 확보에 필요한 조치를 강구하도록 명시하고 있으며, 이밖에 개인정보 수집에 대해서도 인권의 보호를 그 원칙으로 제시하고, 개인정보가 수록된 파일을 비롯한 개인 정보의 안전성 확보에 관한 사항을 구체적으로 제시하고 있으며 개인정보취급자의 의무를 명시하고 부칙에서는 의무 위반자에 대한 처벌도 제시하고 있다.

4.1.4 의료관련 법령

현행 의료관련 법령들은 환자의 보건의료정보 보호에 관한 다수의 규정들을 두고 있다. 보건의료기본법 제12조는 보건의료서비스에 관한 국민의 자기결정권을 규정하고 있으며, 동법 제13조는 보건의료정보의 비밀보호에 대한 규정을 두고 있다.

또한 의료법 제19조는 “의료인은 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료·조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못 한다”라고 하여 의료인에게 환자에 대한 비밀을 준수할 것을 규정하고 있고 동법 제67조는 이 규정에 위반한 경우 3년 이하의 징역 혹은 1천만 원 이하의 벌금에 처하도록 하고 있으나 다만 이 경우에는 고소가 있어야만 공소를 제기할 수 있도록 하였다. 따라서 전염병예방법에 의하여 의사 등이 신고를 하는 경우, 형사소송법 제149조 단서에 의하여 증언을 하는 경우, 개정 민사소송법 제315조에 의하여 증언을 하는 경우, 결핵예방법 제20조에 의하여 의사 등이 결핵환자에 대한 신고를 하는 경우, 후천성면역결핍증예방법 제5조 이하에 의하여 의사 등이 신고를 하는 경우 등을 제외하고는 의료인은 환자에 대한 의료정보의 비밀을 누설해서는 안 된다.

의료법 제20조 (기록 열람 등) 제1항은 “의료인 또는 의료기관 종사자는 다른 법령에서 특히 규정된 경우를 제외하고는 환자에 관한 기록의 열람 사본 교부 등 그 내용확인에 응하여서는 아니 되며 다만 환자, 그 배우자, 그 직계존·비속 또는 배우자의 직계존속, 배우자·직계존·비속 및 배우자의 직계존속이 없는 경우에는 환자가 지정하는 대리인이 환자에 관한 기록의 열람·사본교부 등 그 내용확인을 요구한 때에는 환자의 치료목적상 불가피한 경우를 제외하고는 이에 응하여야 한다.” 고 규정하고 있다.

아울러 동조 제2항은 제1항의 규정에도 불구하고 “의료인은 동일한 환자의 진료상 필요에 의하여 다른 의료기관에서 그 기록, 임상소견서 및 치료경위서의 열람이나 사본의 송부를 요구한 때 또는 환자가 검사기록 및 방사선필름 등의 사본 교부를 요구한 때에는 이에 응하여야 한다.”고 하고 있으며 제3항은 “의료인이 응급환자를 다른 의료기관에 이송할 때에는 환자 이송과 동시에 초진기록을 송부하여야 한다.”고 하고 있어 진료를 위해서는 정보를 공개하도록 의무화하고 있다.

즉 의료정보보호에 대한 기본 근거는 있으나 진료정보의 공개 시 환자에 의한 동의, 정보 접근상의 제한 등에 대한 구체적 명시는 없는 상황이다. 환자에 대한 비밀유지와 관련하여 우리나라에서 독특한 규정으로는 의료법 제19조의2가 규정하고 있는 태아의 성감별 행위 등에 대한 금지 규정을 들 수 있다.

장기등이식에관한법률도 제11조에서 장기등 기증자의 동의에 대한 규정을 두고 있으며, 동법 제27조 제1항은 장기이식의 경우에도 장기기증자 등에 대한 정보의 비밀을 준수할 것을 규정하고 있으나 다만 동조 제2항은 범죄수사를 위한 조사기관이 장기 등의 적출 또는 이식과 관련된 자료를 요청한 경우와 재판과 관련되어 법관이 장기 등의 적출 또는 이식과 관련된 자료의 제출명령을 한 경우에는 예외적으로 정보 제공이 가능하도록 규정하고 있는데 이와 같은 규정은 장기 매매 등 장기이식에 수반될 수 있는 범죄행위에 대한 수사 및 재판에서의 의료정보의 필요성에 기인한다고 할 것이다.

정신보건법 제42조도 정신보건법에 의하여 정신질환자와 관련된 업무를 수행하는 자 혹은 수행하였던 자에 대하여 비밀누설 금지 의무를 부과하는 규정을 하고 있으며 동법 제56조는 이 규정에 위반하여 비밀을 누설한 자에 대하여 3년 이하의 징역 혹은 1천만 원 이하의 벌금에 처하도록

하고 있다.

전염병예방법 제54조의 6도 “보건의료기관·시설 또는 단체 등에서 보건진료 등 전염병 관련 업무에 종사하는 자 또는 종사하였던 자는 업무상 알게 된 타인의 비밀을 누설하여서는 아니 된다”라고 하여 전염병 환자 등에 대한 의료정보의 비밀 보호 규정을 두고 있으므로 전염병의 경우에도 전염병예방법 제4조 이하의 신고와 보고의무에 해당하는 경우를 제외하고는 원칙적으로 의료정보에 대한 비밀이 보호되어야 한다.

또한 후천성면역결핍증예방법 제7조도 “국가 또는 지방자치단체에서 후천성면역결핍증의 예방과 그 감염자의 보호·관리에 관한 업무에 종사하고 있는 자, 감염자의 진단·검안 및 간호에 참여하는 자와 감염자에 관한 기록을 유지·관리하는 자는 재직 중은 물론 퇴직 후에도 정당한 사유 없이 감염자에 관하여 업무상 알게 된 비밀을 누설하여서는 아니 된다”라고 하여 후천성면역결핍증 환자에 대한 비밀누설 금지에 대한 규정을 두고 있으며 동법 제26조는 비밀누설자에 대하여 3년 이하의 징역에 처하도록 하고 있으므로 비록 후천성면역결핍증 환자의 예방 및 관리 등의 목적을 위하여 의사 등에 신고의무(동법 제5조)와 감염자 명부 작성 및 보고 의무(동법 제6조)를 부과하고 있다고 할지라도 원칙적으로 후천성면역결핍증 환자에 대한 의료정보도 개인의 사생활 비밀로서 보호받는다.

의료정보의 대량 입력, 저장 및 처리 등의 정보화가 진행되면 될수록 개인에 대한 정보가 확대·재생산되게 되고 따라서 보호되어야할 개인정보 및 사생활 영역이 점차 확대되고 있는 실정이다. 개정 의료법은 전자의료기록에 대한 보호 규정도 두고 있는바, 제18조의 2 제3항은 “누구든지 정당한 사유 없이 전자처방전에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다”라고 규정하고 동법 제21조의 2 제2항에서는 “누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거

나 누출·변조 또는 훼손하여서는 아니 된다"라고 규정하고 있으며 동법 제66조는 동법 제18조의 2 제3항, 제21조의 2 제3항을 위반한 자에 대하여 5년 이하의 징역 또는 2천만 원 이하의 벌금에 처하도록 하고 있다. 따라서 전자의료기록에 권한 없이 접근하는 경우뿐만 아니라 자료를 유출하는 행위, 전자의료기록의 내용을 변경하거나 하드웨어의 손괴 혹은 컴퓨터 바이러스 감염 등 각종의 방법에 의하여 자료의 내용을 훼손하는 행위도 금지하고 있는 것이다. 이와 같은 규정들은 결국 전자의료기록에 저장되어 있는 개인의 건강에 대한 정보를 보호하기 위한 목적으로 신설된 것이다.

4.2 한국의 의료정보보호 현황

최근 2-3년 동안 보건의료정보화에 발맞춰 병원들의 정보화 투자[65]가 활발히 이뤄지면서 병원의 진료 및 업무 환경이 크게 변화하고 있다. 하지만 병원의 업무와 진료가 정보통신시스템에 의존하는 비중이 높아짐에 따라 병원의 생산성 향상과 경쟁력 확보에 점점 효과를 발휘하는 측면이 커지고 있는 반면, 개인의료정보에 대한 크고 작은 위험도는 더욱 커져가고 있는 실정이다. 즉, 웜이나 바이러스와 같은 사이버 공격이 언제든지 병원 내부 네트워크에 침투해 귀중한 생명을 다루는 환자 진료와 치료 및 서비스 업무에 차질을 주거나 혹은 해킹으로 디지털화된 정보를 빼내거나 위·변조시키는 등 환자의 개인정보자기결정권이 침해될 수 있는 위험요소가 크게 증가되고 있는 것이다. 이에 대하여 병원들은 최근 개인정보보호를 정보화 계획에서 주요하게 다루고 있는 움직임을 보이고 있다. 서울·경기 지역의 500병상 이상의 종합병원들은 대부분 2004년부터 의료정보보호를 적극적으로 검토해왔으며 예산을 확보해 기존 보호 체계를 강화하여 환자의 개인정보보호체계 강화에 나서고 있다.[66]

---

65) OCS(Order Communicaton System, 처방전달시스템), PACS(Picture Archiving and Communications System, 의료정상저장전송시스템), EMR(Electronic Medical Record System, 전자의무기록)뿐만 아니라 ERP, DW, CRM 등 진료와 처방, 병원 행정 및 경영 분야에 각종 정보시스템이 도입되면서 정보통신이 병원 내에서 점차 핵심으로 자리 잡고 있기 때문이다. 이제 병원의 정보통신은 경영의 관점이 접목되어 병원 경쟁력의 잣대로 그 위상을 높이기에 이르렀다.

66) 이유진, "정보보안 투자에 나선 병원, 그 현황과 과제", 컴퓨터월드, 2005, 71-86면

4.2.1 A 병원

환자 내원에서 진료, 처방까지 모든 업무가 완전 정보시스템화된 '디지털 병원'으로 알려진 A병원은 그에 맞는 보안 투자를 꾸준히 진행하고 있다.

A병원은 안티바이러스와 방화벽(인터넷/무선랜존), 침입탐지시스템(IDS)을 운영해 왔으며, 스팸 메일 및 바이러스 메일을 필터링하는 스팸메일 차단 솔루션, 허가받지 못한 전산장비를 통제하는 IP/MAC 통제 시스템, 클라이언트 컴퓨터의 외부 저장장치를 통제하는 통합자원관리솔루션, 웜바이러스 예방과 확상방지를 위한 위한 컴퓨터 방화벽 솔루션 등을 도입해 서버 및 클라이언트 보안 체계를 강화했다.

또한 환자정보보호 측면에서는 웹 digital rights management(DRM) 솔루션을 도입하여 EMR 화면상에서 환자정보가 유출되지 않도록 통제하고 있고, EMR 시스템에 공인인증서를 통한 사용자 인증으로 전자의무기록의 위·변조 방지와 접근제어를 할 수 있다. EMR 시스템의 업무별 메뉴에 대해서는 개인별/부서별/그룹별로 해당 업무와 관련된 권한만을 부여하는 차등 관리를 하고 있다. 전자의무기록 열람시에는 열람사유를 반드시 남겨 주기적으로 접속 로그를 분석하고 비인가된 열람에 대한 감사를 실시하여 사후조치를 하는 체계를 마련하고 있다.

또한 최근 2년동안 보안컨설팅 전문업체의 전문 컨설턴트를 통해 주기적으로 시스템 및 네트워크 전반의 보안 취약점 점검과 모의해킹을 실시하고 문제를 해결해왔으며, 2006년 8월부터는 국정원 산하 국가사이버안전센터와 보안관제망을 연동하여 실시간 모니터링을 시행하고 있다.

2006년에는 각 보안장비 및 솔루션을 통한 EMS(Enterprise Security

Managemanet)을 구축하여 보안관리의 효율성을 향상시켜 사고대응시간을 단축시킬 수 있는 체계를 마련하였다.

또한 일반 시스템 장애(DB 문제, H/W 장애 등)에 대한 대응절차를 성문화하여 마련하고, 장애대응 모의훈련도 실시하고 있다. 아직은 연 1회이지만, 내년부터는 분기별 1회로 늘릴 계획이다. 시스템 장애는 진료부원장을 팀장으로 하는 장애 대응팀이 구성되어 체계적으로 관리, 대응하고 있다. 재해로 인한 장애(전쟁,테러,홍수,화재 등)로 시스템 운영실이 완전히 기능이 마비되어 정상 운영을 지원할 수 없는 경우 이를 지원하도록 하는 원격지 DR(Disaster Recovery) 센터는 아직 없으나, 곧 3차에 걸친 프로젝트를 진행할 계획이다.

그 외에 중요한 데이터는 일일/주간/월간 주기로 백업을 받고 있으며, 원격지에 소산하여 보관도 하고 있다.

구 분	A 병원 적용내용
통신망 및 네트워크 보안	- 무선 LAN 보안 - 방화벽, 침입탐지시스템(IDS), 폐쇄적 광역통신망 - 네트워크 장비/케이블 이중화 - 상시 모니터링 - 국가사이버안전센터와 보안관제망 연동
시스템 접근통제	- 복합인증 (스마트카드) - 역할별 메뉴 구성/권한(개인별,부서별,직종별,업무별) - 인사발령과 ID관리 자동연계:(퇴직처리시 사용제한)
보안 관리	- 병원 보안규정/정책 - 주기적인 보안점검(월별) - 보안서약서(개인별/시스템 사용 ID, 인증카드 발급) - 통신보안전문가(CERT) 육성, 정기적 교육
응용프로그램 및 시스템개발 보안	- 6자리이상의 영,숫자 혼합 비밀번호 - 주기적 비밀번호 변경 - 일정시간 미사용시 자동 Log-off - 출력/조회시 Logging
시스템운영 보안	- 제3자의 정기적 점검 - 백신, Spyware (PC-안철수연구소 V3/spyzero, 메일-Sopos) - PC 원격점검 및 제어
암호학	- 공인인증서 - PKI기반 전자서명(서명 이미지 표시) - 비밀번호 암호화
사업지속계획 및 재난복구계획	- 재난복구계획 수립(절차 마련, 시스템구성 계획 중) - 주기적 모의 훈련 (장애대응모의훈련만, 재난훈련없음) - 백업테이프 소산 보관
물리적 보안	- 제한된 인가자 출입, logging - 출입 보안 (스마트카드)

표 4 A 병원의 안전보호 관리

4.2.2 B 병원

B병원은 환자정보의 보호를 위하여 보안분야에서는 방화벽 이중화와 안티스파이웨어, 보안자가진단을 위한 취약점 분석 스캐너 도입하고 있다. 또한 B병원은 그룹 차원에서 외부 침입에 대한 1차 방어체제를 이미 구현했으며, 내부 병원 망에서도 안티바이러스와 방화벽, 침입탐지시스템(IDS)을 별도 운영하고 있다. 그룹 정보보안센터의 보안 기준을 적용할 뿐만 아니라 통합 보안 관제서비스를 받고 있으며, 내부 망과 사이버 인터넷 망에 연3회 주기적으로 보안 감사를 받고 있다. 또 병원 자체적으로 매월 4일을 '안전보안 점검의 날'로 지정해 보안 및 안전 점검을 실시하고 있다.

모바일 진료시스템에는 복합인증(ID/ 패스워드, 폰넘버체크)과 데이터 암호화를 적용하고 있으며, EMR에 공인인증서 기반 인증과 공개키 기반구조(PKI)[67]의 전자서명 및 암호화를 실시하고 있다. 특히 EMR에는 역할 기반 접근제어(RBAC)에 의거해 사용자 역할별 접근 메뉴를 차별화해 접근제어 및 권한관리를 실시하고 있다. 또한 주요 정보 조회/출력 시 사용자와 조회시간, 조회 IP 등의 기록을 남겨 정보유출에 대비하고 있다.

67) 인터넷 사용자가 보유한 암호를 이용해 거래자 신원을 확인하는 방식

구 분	B 병원 적용내용
통신망 및 네트워크 보안	- 무선 LAN 보안 (단말인증) - 가상사설망(VPN) (가정간호) - 방화벽, 침입탐지시스템(IDS), 폐쇄적 광역통신망 - 네트워크 장비/케이블 이중화 - 상시 모니터링
시스템 접근통제	- 복합인증 (스마트카드) - 역할별 메뉴 구성/권한:(필요시) 개인별 메뉴/권한 - 인사발령과 ID관리 자동연계:(퇴직처리시 사용제한)
보안 관리	- 병원 보안규정/정책 - 주기적인 보안점검 - 보안서약서(개인, 매년) - 통신보안전문가(CERT) 육성, 정기적 교육
응용프로그램 및 시스템개발 보안	- 6자리이상의 영,숫자 혼합 비밀번호 - 주기적 비밀번호 변경 - 일정시간 미사용시 자동 Log-off - 출력/조회시 Logging
시스템운영 보안	- 통합관제 서비스 - 제3자의 정기적 점검 - 백신, Spyware - PC 원격점검 및 제어
암호학	- 공인인증서 및 PKI기반 전자서명 - 비밀번호 암호화
사업지속계획 및 재난복구계획	- 재난복구계획 수립 - 주기적 모의 훈련 - 백업테이프 소산 보관
물리적 보안	- 전산실 3차 시건 - 제한된 인가자 출입, logging - CCTV 및 출입 보안 (스마트카드)

표 5 B 병원의 안전보호 관리

4.2.3 C 병원

대규모 정보통신예산을 투입하면서 네트워크와 시스템을 개편하고 EMR구축까지 완료한 C병원은 통신망 및 네트워크 보안을 위하여 방화벽, IDS, IPS 및 무선랜 보안, 바이러스/침입 차단시스템과 스팸메일 차단, 단말기보안, 문서 및 웹의 정보유출방지 시스템, 폐쇄적 WAN, 상시모니터링 등 보안시스템을 대거 구축해 네트워크 및 시스템 단의 내·외부 방비체계를 마련했다. 또한 전사적 통합 보안 서비스를 내년 도입하여 더욱 체계적인 보안 서비스를 실시할 예정이다.

시스템접근 통제를 위하여 일반적으로는 IC chip 이 내장된 스마트카드를 사용하고 있으며 특별히 장기 이식실 등 주요 facility는 지문인식 인증 시스템을 사용하고 있다. 현재는 총무과 DB를 제외한 인사발령과 ID 관리를 자동으로 연계하고 있으며 퇴직시 ID 사용을 제한하고 있다. EMR과 관련하여는 역할별로 메뉴를 구성하고 권한을 부여하고 있다.

또한 별도로 의료정보보호를 위한 보안규정/정책 등을 마련하여 운영하고 있으며 신입사원 발령시 직원들에게 보안서약서를 작성하도록 하고 있다. 현재 보안점검 및 의료정보보호 교육은 비정기적으로 이뤄지고 있으며 앞으로 보안 전문가(CERT)를 육성할 예정에 있다.

현재 4자리의 비밀번호를 사용하고 있으나 시리얼번호를 제한하고 있고, 1달을 주기로 비밀번호를 변경하도록 하고 있다. 또한 작업 환경에 따라 30초에서 30분 이상 미사용시 자동 로그 오프 되도록 설정하고 있다. 그 밖에 재난 복구에 대비하여 DR 센터를 운영하고 있다는 점 및 지문 인식을 이용하여 전산실의 출입을 제한하고 있다는 점이 특이할 만하다.

구 분	C 병원 적용내용
통신망 및 네트워크 보안	- 무선 LAN 보안 - 방화벽, 침입탐지시스템(IDS), IPS - 폐쇄적 광역통신망 - 네트워크 장비/케이블 이중화 - 상시 모니터링 - VPN
시스템 접근통제	- 복합인증 (IC 칩 내장 스마트카드, 장기이식실-지문) - 역할별 메뉴 구성/권한 - 인사발령과 ID관리 자동연계:(퇴직처리시 사용제한)
보안 관리	- 병원 보안규정/정책 - 보안서약서(신입직원 발령시)
응용프로그램 및 시스템개발 보안	- 4자리의 비밀번호, 시리얼번호 제한 - 주기적 비밀번호 변경(1달) - 일정시간미사용시자동Log-off (30초-30분customizing) - 출력/조회시 Logging
시스템운영 보안	- 제3자의 비정기적 점검 - 백신, Spyware (스파이제로-안랩 제품) - PC 원격점검 및 제어
암호학	- 공인인증서 - PKI기반 전자서명 - 비밀번호 암호화 (policy 서버에 저장)
사업지속계획 및 재난복구계획	- 재난복구계획 수립 - 주기적 모의 훈련 - 백업테이프 소산 보관 - DR 센터 운영
물리적 보안	- 제한된 인가자 출입 - 출입 보안 (지문 인식)

표 6 C 병원의 안전보호 관리

4.2.4 D 병원

작년 대규모 신축 공사를 하고 새로운 진료체제를 갖춘 D 병원은 병원 전체가 처음 출범부터 EMR을 완벽하게 도입하여 통합적인 정보 시스템을 의료 행위에 제공하고자 하였다.

통신망 및 네트워크 보안을 위하여 방화벽, 침입탐지시스템(IDS) 및 네트워크 장비/케이블 이중화를 구현하였으며 시스템운영보안 측면에서는 바이러스 및 스팸메일을 차단하기 위하여 다양한 백신과 spyware를 운영하고 있다.

특히 D 병원은 시스템접근 통제 차원에서 병원의 의사들에게 모두 지문인식 기능이 탑재된 마우스로 PC를 사용하게 함으로써 환자의 의료정보 접근에 있어 신원확인시스템으로 ID, Password 외에 지문인식을 요구하는 강력한 보호를 하고 있다. 또한 환자 진료기록의 접근권한 관리에 있어서도 진료, 간호, 원무 및 보험청구 등 업무별로 분류하여 메뉴를 차별하고 있으며 통합시스템의 메뉴를 최대한 단순화 함으로써 권한 관리를 더 엄격히 하고자 하였다. 또 진료정보의 출력 및 조회 시 기록이 남도록 하여 보관하고 있으며 3시간 이상 미사용시 자동 로그 오프되도록 관리하고 있다. 그 밖에 공인인증서, PKI 기반전자서명 사용은 물론이며 8 자리의 비밀번호를 사용하여 암호화하고 있다. 관리적 보안으로 엄밀히 성문화된 보안정책을 수립하고 있지는 않으나 자체적인 규칙 하에 환자정보보호에 주의를 기울이고 있다.

구 분	D 병원 적용내용
통신망 및 네트워크 보안	- 무선 LAN 보안 - 방화벽, 침입탐지시스템(IDS), 폐쇄적 광역통신망 - 네트워크 장비/케이블 이중화 - 상시 모니터링
시스템 접근통제	- 복합인증 (ID/지문인식) - 역할별 메뉴 구성/권한 - 인사발령과 ID관리 자동연계:(퇴직처리시 사용제한)
보안 관리	- 주기적인 보안점검 - 보안서약서(ID발급시) - 정기적 교육(일상적인 교육의 일부분으로)
응용프로그램 및 시스템개발 보안	- 8자리의 영,숫자 혼합 비밀번호 - 3시간이상 미사용시 자동 Log-off - 출력/조회시 Logging (출력자 및 조회자 조회 불가)
시스템운영 보안	- 제3자의 정기적 점검 - 백신, Spyware - PC 원격점검 및 제어
암호학	- 공인인증서 및 PKI기반 전자서명 - 비밀번호 암호화
사업지속계획 및 재난복구계획	- 백업테이프 소산 보관
물리적 보안	- 제한된 인가자 출입(전산실)

표 **7** D 병원의 안전보호 관리

4.2.5 E 병원

E 병원에서는 2005년 11월 유비쿼터스 환경의 병원을 설계하고 구축하여 성공적으로 통합의료정보시스템을 가동하고 있다. 특히 의료정보의 보안을 환자의 사생활 보호 측면 뿐 아니라, 법적 분쟁 시 유일하게 진료기록의 보존 및 변조를 방지하고 활용하기 위한 중요한 요소로 인식하고 정보 보안 정책 수립을 통한 의료정보보호에 박차를 가하고 있다.

E 병원은 통신망 및 네트워크 보안을 위하여 무선LAN 보안, 방화벽 및 폐쇄적 WAN을 구현하고 네트워크 장비/케이블을 이중화하고 상시 모니터닝을 하고 있다. 시스템 운영 보안을 위하여 꾸준히 제3자의 정기적 점검을 받고 있으며 **symantec**과 **hauri** 등 백신 및 **spyware**를 구현하고 PC 원격점검 및 제어도 이루고 있다.

시스템 접근 통제를 위하여 스마트 카드를 통한 복합인증을 요구하고, 퇴직 처리 시 ID가 자동 삭제되도록 구성하고 있으며, 환자 진료기록의 접근권한 관리에 대하여 EHR 접근권한 관련 정책과 직종별 접근 원칙을 바탕으로 하여 관련 업무와 관련 환자를 기준으로 권한을 설정[68]하였다. 또한 보안정책을 확립하여 매월 보안점검을 하고 있으며 네트워크,ID,인증서 발급시 보안서약서를 받고 있다. 작년 개원 이후 현재까지 1회에 걸쳐 장애에 대비한 모의 훈련을 실시하였으며 앞으로도 정기적으로 장애 및 재해에 대비한 모의 훈련을 실시할 예정이다. 그 밖에 전산실에 제한된 인가자만 출입할 수 있도록 하고 있으며 특히 CCTV및 정맥 인식을 통한 출입 보안을 이루고 있는 점이 주목할 만하다.

---

68) 김용욱 외, “**Essential Elements of EHR System**" 군자출판사,

구 분	E 병원 적용내용
통신망 및 네트워크 보안	- 무선 LAN 보안 (단말인증) - 가상사설망(VPN) (의료정보실만 사용) - 방화벽, 침입탐지시스템(IDS), 폐쇄적 광역통신망 - 네트워크 장비/케이블 이중화 - 상시 모니터링
시스템 접근통제	- 복합인증 (스마트카드) - 역할별 메뉴 구성/권한:(필요시) 개인별 메뉴/권한 - 인사발령과 ID관리 자동연계:(퇴직처리시 사용제한)
보안 관리	- 병원 보안규정/정책 - 주기적인 보안점검 (매월) - 보안서약서(네트워크, ID, 인증서 발급시,)
응용프로그램 및 시스템개발 보안	- 6자리이상의 비밀번호(초기 9자리) (정기적, 주기적 변경 가능) - 출력/조회시 Logging (출력:의무기록팀만 가능, 조회:사용자별 관리)
시스템운영 보안	- 제3자의 정기적 점검 - 백신, Spyware (symantec, hauri) - PC 원격점검 및 제어
암호학	- 공인인증서 및 PKI기반 전자서명 - 비밀번호 암호화
사업지속계획 및 재난복구계획	- 재난복구계획 수립 (OCS/EMR) - 주기적 모의 훈련 - 백업테이프 소산 보관
물리적 보안	- 전산실 시건 - 제한된 인가자 출입, logging (전산실 한정) - CCTV 및 출입 보안 (정맥 인식) - DR 센터 운영

표 8 E 병원의 안전보호 관리

4.2.6 F 병원

외래진료부터 병동진료와 간호업무에 이르기까지 모든 진료환경에 자체 개발한 전자의무기록(EMR)를 도입하여 사용하고 있는 F병원은 통신망 및 네트워크 보안을 위하여 업무망과 인터넷망을 물리적으로 분리하여 구축하여 사용하고, 방화벽 구축, IPS 관리, VPN 사용제한, 상시 모니터링 등을 실시하고 있다.

또한 시스템 접근 통제를 위하여 스마트카드 사용하다 KMS(key manager server) 방식으로 교체하여 사용하고 있으며 CLASS(업무그룹), GRADE(단위업무), PROGRAM_ID(단위프로그램), 사번 등으로 권한을 분류하여 접근을 제한하고 있다. 병원 자체적으로 보안규정을 마련하는 것은 물론이며 특별히 정보보호위원회를 구성·운영하고 개인정보 관리책임자도 임명하고 있다. 전 직원을 대상으로 보안 서약서를 받고 있지는 않지만 대량의 자료를 가공하여 이용하는 자에 대해서는 따로 보안 서약서를 작성하도록 하고 있다.

F 병원은 비밀번호 방식도 기존에 6자리에서 8자리 방식으로 확장하여 사용하고 있으며 특히 영, 숫자, 특수문자를 포함하도록 하고 있다. 또한 의료정보의 출력은 의무기록팀에서만 가능하도록 제한하고 있으며, 출력요청자의 정보와 용도, sheet종류 등의 출력 history를 남기도록 하고 있다.

그 밖에 암호학 관련 사항으로 공인인증서 및 전자인증서버(KMS) 방식 전자서명을 사용하고 있으며 비밀번호는 암호화하여 저장하고 있지만, 전자서명 비밀번호의 생성 규칙은 open되어 있고, 업무에 적용 시에는 인사사번의 비밀번호와 조합하여 사용하도록 하고 있다.

시스템 운영 보안에 관한 사항으로는 하우리(바이로봇)를 보안 솔루션으로 채택하고 있으며 전산실 외부의 특수 캐비넷을 이용해 백업 테이프를 소산하여 보관하고 있는 점이 특이할 만하다.

구 분	F 병원 적용내용
통신망 및 네트워크 보안	- 무선 LAN 보안 (단말인증) - 가상사설망(VPN)사용 제한 - 방화벽, IPS - 업무망과 인터넷망을 물리적으로 분리·구축 사용 - 상시 모니터링
시스템 접근통제	- 복합인증 (KMS-key manager server) - 역할별 메뉴 구성/권한: CLASS(업무그룹), GRADE(단위업무), PROGRAM_ID(단위프로그램), (사번) - 인사발령과 ID관리 자동연계:(퇴직처리시 사용제한)
보안 관리	- 병원 보안규정/정책 - 정보보호위원회 구성 - 보안서약서(특정인)
응용프로그램 및 시스템개발 보안	- 8자리의 영,숫자,특수문자 혼합 비밀번호 - 출력/조회시 Logging - 의무기록팀만 의료정보출력가능 (출력요청자의 정보와 용도, sheet종류 등 기록)
시스템운영 보안	- 백신, Spyware (하우리(바이로봇))
암호학	- 공인인증서 - 전자인증서버(KMS) 방식 전자서명 - 비밀번호 암호화
사업지속계획 및 재난복구계획	- 백업테이프 소산 보관 (전산기계실 밖에서 특수 캐비넷을 이용)
물리적 보안	- 제한된 인가자 출입 - 출입자 명부 작성

표 9 F 병원의 안전보호 관리

4.3 소결

4.3.1 한국의 의료정보보호 법제도 분석

의료정보의 접근 및 활용의 폭이 넓어질수록 환자 개인정보의 보호 차원에서 의료정보에 대한 더욱 엄격한 관리가 필요하다. 의료정보에 대한 보호 조치가 미흡한 상태에서의 의료정보화는 그 정보의 내실을 기대할 수 없기 때문이다. 그럼에도 불구하고 현행 의료법에서는 의료정보를 충분히 보호하고 있다고 보기 어렵다. 아직 정보화가 완성되지 않고 진행 중인 단계에서 어쩌면 당연한 일일 수도 있겠으나, 상당 정도로 의료 정보의 전산화가 진행되어 있는 현 상태에 있어서도 현행 의료법 및 일반법의 추상적인 규정에만 의지하여 의료정보보호를 논하는 것은 너무 안이한 자세이다.

주지하다시피 우리나라는 현재 의료정보가 침해될 경우 이를 규제할 마땅한 법규범이 없는 실정이다. 의료법상의 비밀누설 금지조항은 의료인의 비밀준수 의무를 규정하고 있으나 동 조항을 의료정보 전반에 적용하기에는 무리가 있다. 의료정보의 전산화로 인하여 의료정보는 이제 더 이상 의료인들만의 취급 정보가 아니게 되었으며, 의료정보는 더 이상 의료법상에 열거되어 있는 좁은 의미의 의료정보만을 의미하는 것이 아니게 되었기에 의료인의 비밀 준수 의무만으로 그 보호를 충족시키는데 한계에 다다른 상태이다.

정보의 이용과 관련한 규정으로는 공공기관의 정보공개에 관한 법률 제10조에서 원칙적으로 개인정보 파일의 보유 목적 외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하지 못하도록 규정하고, 다만 정보주체나 제3자의 권리와 이익을 부당하게 침해할 우려가 있을 경우를 제외하고

소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우는 이용이 가능하도록 규정되어 있다. 그러나 공공기관의 개인정보 보호에 관한 법률의 적용범위가 그 대상을 공공기관으로 한정하고 있으며, 정보주체의 동의를 요하지 않는 '상당한 이유'의 범위가 명확하지 않다는 점에서 한계를 가지고 있다.[69]

또한 현재 민간분야에서 실제적으로 개인정보기본법의 역할을 하고 있는 정보통신망이용촉진및정보보호등에관한법률의 경우도 그 적용 대상이 정보통신서비스제공자에 한정되어 의료기관에 의한 개인정보침해가 발생할 경우 관련 규정들을 적용하는 데에는 한계가 있으며, 정보통신에 관한 법령과 의료관련 법령에서 각각 개인정보 보호규정이 존재함으로써 정보통신의 특수성과 의료의 특수성을 적절하게 법제화하지 못하고 있는 실정이다.

즉, 현재 우리나라 의료정보보호 현황은 의료정보 보호에 대한 종합적이고 구체적인 규정이 없을 뿐 아니라 개인정보보호와 보안에서 요구되는 내용을 충실히 포함하는 지침이나 구체적 검토 없이 정보보호를 진행하고 있는 실정이므로, 정보화된 의료정보의 이용 및 활성화에 따라 의료정보보호 및 의료정보활용이라는 두 가지 목적을 아우를 수 있는 통일되고 구체적인 법제도의 마련이 요구된다.

69) 김정은, "진료정보공동활용현황 및 촉진 방향 자료", 2003

4.3.2 한국의 의료정보보호 현황 분석

구 분		A병원	B병원	C병원	D병원	E병원	F병원
통신망 및 네트워크 보안	무선 LAN 보안	○	단말인증	단말인증	○	○	
	방화벽	○	○	○	○	○	○
	IDS	○	○	IDS/IPS	○	IPS	IPS
	폐쇄적WAN	○	○	○	○	○	
	네트웍장비/케이블 이중화	○	○	○	○	○	○
	상시 모니터링	국가사이버안전센터와 연동	○	○	○	○	○
시스템 접근통제	복합인증	스마트카드	스마트카드	스마트or 지문	지문인식	스마트카드	KMS
	역할별 메뉴 구성	개인별,부서별,직종별,업무별	필요시 개인별	역할별	○	○	업무별,단위위업무별,프로그램,사번
	인사발령과 ID관리 자동연계	퇴직처리시	퇴직처리시	총무과DB제외	퇴직시	인사DB와 연계	○
보안 관리	보안규정/정책	○	○	○		○	○(보호위원회)
	주기적인 점검	매월	○	비정기	○	매월	
	보안서약서	개인별, ID	개인, 매년	신입 발령시	ID 발급시	ID,인증서	특정
	CERT 육성	○	○	예정			
	정기적 교육	○	○	비정기	△		
응용 프로그램 및 시스템 개발 보안	비밀번호	6자리이상의 영,숫자 혼합	6자리이상의 영,숫자 혼합	4자리	8자리	초기9자리,최초 로그인시 반드시 변경	8자리,영·숫자·특수문자
	주기적 비밀번호 변경	○	○	1개월			
	일정시간 미사용시 자동 Log-off	○	○	30초-30분	3시간	30분	
	출력/조회시 Logging	○	○	○	○	출력:의무기록팀만 가능 조회:사용자별	의무기록실만 출력 가능
시스템 운영 보안	통합관제 서비스	○	○				
	제3자의 정기적 점검	○	○	비정기	○	○	
	백신, Spyware	○	○	○	○	○	○
	PC 원격점검 및 제어	○	○	○	○	○	예정
암호학	공인인증서 및 PKI기반 전자서명	○	○	○	○	○	○
	비밀번호 암호화	○	○	○	○	○	○
사업지속계획 및 재난복구계획	재난복구계획	절차 마련	○	○		OCS/EMR	
	주기적 모의 훈련	장애대응 훈련	○	○		○	
	백업테이프 소산보관	○	○	○	○	○	○
물리적 보안	제한된 인가자 출입	○	○	○		○	○
	logging/CCTV		○			○	
	출입 보안	○	스마트카드	지문인식	전산실만	정맥인식	

표 10 병원의 안전보호 관리 비교

최근 병원들의 의료정보화가 활발히 추진되면서 대형 병원들을 중심으로 환자의 의료정보보호를 위한 보안 대책의 설립 및 운용이 활발히 진행되고 있음을 앞서 살펴보았다. 이들 병원들은 일찍이 의료정보의 보호가 환자와 의료인간의 신뢰 확보 및 의료서비스의 질 향상에 차지하는 중요성을 인식하고 의료정보화와 동시에 의료정보보호를 위한 보안 유지에 앞장서 왔다. 비록 정부 차원에서의 구체적인 지침이 존재하지 않아 병원들 간에 약간의 차이는 있으나 전반적으로 보안 유지를 위하여 다양한 방법을 강구하고 있음을 알 수 있다. 특히 기술적 측면의 보안 관리인 통신망 및 네트워크 보안, 시스템 운영 보안 등에 관한 사항들은 병원 업무에 직접적인 침해를 줄 수 있는 부분이기 때문에 모두 충실히 운용하고 있음을 볼 수 있다. 그리고 공인인증서 및 PKI 기반 전자서명과 비밀번호 암호화 관련 사항도 법적으로 요청되고 있는 사항으로서 모두 실시되고 있었다. 그러나 관리적 보안 사항인 보안정책과 재난복구계획의 마련, 보안서약서 및 보안 교육에 대한 운영은 소홀한 실정이며, 물리적 보안 사항인 DR 센터 마련 및 출입 통제도 제한적으로 이루어지고 있었다.

그 밖에 환자의 의료정보와 직접적으로 관련된 시스템 접근 통제에 관하여서는 이들 병원이 모두 의료정보보호에 대한 중요성을 인식하고 각 병원별로 역할별·업무별 메뉴를 구성하여 접근을 제한하는 한편, 스마트 카드 및 지문인식 시스템을 도입하여 권한 없는 자의 접근을 차단하고자 노력을 기울이고 있었다. 이는 정보에 대한 접근을 처음부터 차단함으로써 실질적인 정보 침해의 위험을 감소시키는 일이기에 이러한 병원들의 자체적인 노력은 매우 고무적인 일이라 할 것이다.

앞서 살펴 본 바와 같이, 일부 대형병원들이 환자 정보 유출 방지를 위하여 각 기술적, 관리적, 물리적, 애플리케이션 보안에 나름의 노력을 기울이고 있기는 하나, 기술적 관리에 관한 사항과 사용자 인증체계와 전자서

명 및 암호화를 제외한 관리적, 물리적 관리는 그 운용이 미흡한 상태이며 어플리케이션 측면의 관리도 오로지 병원들의 자발적인 인식에 의해 이루어지고 있기 때문에 통일되어 있지 않다는 문제점이 있다. 또한 이들 병원을 제외한 다수의 병원들이 보안에 대한 인식을 새로이 하고 앞다투어 이 문제를 해결하기 위한 움직임을 보이고 있지만 여전히 대부분의 병원들은 이제 겨우 초보적인 보안 체계를 갖춰 나가고 있다고 해도 과언이 아니기 때문에 이에 대한 대책이 필요하다. 이는 병원 환경에 대한 보안 전문가가 부족하고 병원 환경을 제대로 이해해 가이드를 제시할만한 곳이 많지 않다는 현실과 막대한 비용이 소요된다는 부담에 따른 당연한 결과일지도 모른다. 그럼에도 불구하고 환자의 의료정보보호는 반드시 이뤄져야 할 의무이다. 따라서 이러한 의료정보보호의 필요성에 대한 욕구를 충족하는 한편, 공공의 성격을 띠는 의료기관의 부담을 완화하기 위하여 정부 차원의 의료정보보호를 위한 가이드라인 제시나 보안 기준 및 특화된 법규 체계의 마련이 더욱 필요하다고 할 것이다. 정부는 의료정보 보호를 위한 정부차원의 기준을 명확히 하고 관련 보안 법규 등 급변하는 정보화 환경에 맞는 법률의 마련과 행정적 규제를 적기에 시행할 필요가 있다.

제5장 의료정보보호의 쟁점 및 개선방안

의료정보는 궁극적으로는 개인에 대한 정보이기 때문에 전통적인 프라이버시권의 옹호 아래 개인의 사생활보호의 차원에서 헌법적 보호를 받아왔다. 그러나 최근에 이루어진 컴퓨터 및 정보통신의 발달로 말미암아 전통적 프라이버시권의 범주에서 정보에 대한 접근 차단 및 사생활의 비밀로 보호되던 정보 개념은 그 의미를 상실하였다. 절대적인 사생활권의 비호를 받는 정보 보호라기보다는 이제는 오히려 공적 성격을 지니는 개인정보의 이용을 통한 효용을 창출케 하면서 적극적으로 자기정보 내지 개인정보에 대한 흐름을 감시 및 통제하는 개인정보통제권의 영역에서 개인정보보호에 대한 논의가 이루어져야 한다. 개인정보통제권은 그 내용으로 정보주체와 정보취급자에게 일정한 권리 및 의무를 부과한다. 따라서 준공공재의 성격을 갖는 의료정보도 이러한 권리·의무 관계를 중심으로 보호에 대한 논의가 이루어져야 한다. 그러나 국내의 경우, 의료정보의 활용성이 커진다는 것은 곧 집적된 의료정보에 대한 침해 가능성도 비례하여 증가한다는 것이기에, 정보들의 보호 필요성이 증대되고 있음에도 불구하고, 현행 의료법에서 의료정보를 충분히 보호하고 있다고 보기 어려우며 또한 현실을 반영하는 기타 제도적 입법도 충실히 이루어지지 않고 있는 상태이다. 본 장에서는 의료정보보호 및 이용에 관한 원칙과 기준을 바탕으로 개인정보통제권의 내용으로 도출된 권리 및 의무 관계에 따라 의료정보 보호를 위한 법적 쟁점을 살피고 순기능적 정보 이용을 위한 의료정보의 제도적 보호 방안을 모색하고 그 개선안을 제시하고자 한다.

5.1 의료정보보호의 법적 쟁점사항

5.1.1 의료정보주체의 권리

개인정보통제권으로부터 도출되는 의료정보주체의 권리·의무의 내용으로는 타인에게 알리고 싶지 않다고 생각하는 것이 정당한 일정한 사적인 의료정보에 관하여 개인정보의 수집 및 획득, 개인정보의 보유 및 이용, 개인정보의 열람 및 제공, 개인정보의 침해 각각의 단계에서 정보주체에 의한 통제의 권리보장을 요구함과 동시에 이러한 권리를 실효적으로 확보하기 위하여 개인정보의 열람청구권 및 정정청구권을 도출하며 나아가 정보취급자에게 정보수집의 목적이외에 사용하지 않거나 비밀유지 및 정보보안에 철저할 것을 요구한다. 먼저, 의료정보주체의 권리 내용은 각 단계별로 다음과 같다.

환자의 권리		내 용
수집 통제권	정보의 수집	1. 명확한 의료정보 수집 목적 2. 적절한 의료정보 수집 범위 3. 의료정보 수집의 방법 -
	정보의 이용	1. 의료정보의 이용목적 제시 2. 의료정보 이용의 동의 3. 의료정보 이용기간 4. 의료정보의 이용제한
보유 통제권		1. 의료정보 접근권 2. 의료정보 정정청구권
이용·제공 통제권		1. 중단 청구권 2. 추가적 동의권 3. 개시 고지권 4. 손해배상청구권[70]

표 11 의료정보주체관련 법적 권리

5.1.1.1 수집통제권

수집통제권이란 자신에 관한 정보의 흐름을 원칙적으로 정보주체의 의사에 따르도록 하기 위하여 의료정보의 획득 및 이용에 있어서 충분하고 적절한 절차에 의한 설명을 받고 이에 기초하여 수집에 대한 동의를 할 권리[71]를 말한다. 즉, 수집통제권을 구성하는 권리는 수집동의권 및 그 전제조건이 되는 설명청구권이라 할 수 있다. 의료행위를 통해서 획득되어지는 것이든 혹은 연구행위의 일환으로 획득되어지는 것이든 특정 개인의 의료정보를 획득하는 경우에는 그 의료정보 주체의 동의[72]를 얻는 것이 원칙이다. 만일 이러한 정보주체의 동의를 얻지 않고서 개인정보를 수집하려면 반드시 법률에 그 근거 규정이 있어야 한다.

정보주체의 동의는 정보주체의 자유로운 결정에 기초한 것이어야 한다. 그러기 위해서는 정보주체가 그 정보의 수집에 따라 발생할 수 있는 여러 문제점들을 충분히 이해할 수 있는 상황이 전제되어야 한다. 따라서 그 수집에 앞서 수집사실의 고지와 명시적인 수집목적의 제시가 필요하고, 수집된 개인정보의 처리와 이용 등에 대한 구체적인 안내[73]가 있어야 한다. 여기에는 정보처리의 목적, 정보관리자와 정보수집자의 신원, 수집거부에 따르는 피해, 향후의 정보처리과정에 있어서 정보주체의 관여권 등에 대한 충분한 고지와 설명이 요구된다.

---

70) 김준호, "민법강의", 법문사, 2006, 1545-1576면

71) 권건보, 앞의 책, 35면

72) 보건의료기본법 제12조는 모든 국민은 보건의료인으로부터 자신의 질병에 대한 치료방법·의학적 연구대상 여부·장기 이식 여부 등에 관하여 충분한 설명을 들은 후 이에 관한 동의 여부를 결정할 권리를 가진다고 규정한다

73) HIPAA 프라이버시규칙에서는 각 의료기관이 환자의 의료정보취급방침을 환자에게 통지하도록 하고 있다. 특히 2002년 규칙개정에 의해 환자가 이 통지를 받았다는 것을 인정하는 서면을 남길 것을 의무화 하였다.

수집통제권의 다른 내용으로 민감한 개인정보의 수집금지가 있다. 개인에게 대단히 민감한 개인정보의 경우, 수집 자체에 의해 인간 내면의 본질적인 자유의 내용을 침해할 가능성이 높기 때문에 수집 단계부터 제한할 필요가 있다. 따라서 건강상태, 성생활 및 유전정보 등과 같은 민감한 의료정보는 정보주체의 명백한 동의가 없는 한 그 수집을 원칙적으로 금지[74]해야만 한다.

5.1.1.2 보유 통제권

보유 통제권의 내용으로는 의료정보 접근권 ,의료정보 정정청구권 및 삭제·차단 청구권이 있다.

정보주체는 자신에 관한 정보를 보유하고 있는 자에 대하여 그 정보의 열람을 청구[75]할 수 있고 당해 정보의 보유자는 특별한 사유가 없는 한 그 열람을 허용하여야 한다.[76] 우리나라의 경우 보건의료기본법 제11조에는 보건의료에 관한 알권리에 대해서, 모든 국민은 관계 법령이 정하는 바에

---

74) 공공기관의개인정보보호에관한법률도 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우를 제외하고는 사상 신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집할 수 없도록 하고 있다.

75) 미국의 경우 진료기록의 소유권은 그 정보를 작성한 의료기관에 있는 것으로 인정되고 있으나 그 물적 매체에 있는 환자 정보의 내용은 환자의 소유라고 법적으로 보장되고 있으므로 정보의 소유권자로서 환자는 해당정보의 유출 및 사용에 대해서 알고 그 이용 여부를 결정 내릴 권리가 있다. 좀 더 적극적인 의미의 소유권으로 환자는 자신의 진료기록에 대한 접근권을 가진다는 의미로 많은 논란 끝에 미국의 현행법이나 판례에 의해서 인정받게 되었다. 1984년 미국에서 제정된 정보보호법(The Data Protection Act)은 컴퓨터에 저장된 자신의 기록에 접근할 권한을 인정하였고 이는 의료정보의 경우에도 해당될 수 있는가 하는 문제가 제기되었다.
1991년 11월 의무기록접근에 관한 법안(The Access to Health Records Bill)이 통과가 되었고 환자 자신에게 심각한 해를 미치거나 정보제공자를 보호할 필요가 있는 경우를 제외하고는 환자들의 접근권한을 인정해 주고 있다(Britten N et al, (1991). Consultants' and Patients' View About Patient to their General Practice Records. Journal of the Royal Society of Medicine. 84. 284-287.) 그러나 이러한 환자자신의 진료기록에 대한 접근권은 법조문상 "합법적인 접근", "선의의 동기"와 같은 조건을 부여함으로써 실제 운용에 있어서는 접근을 제한할 수 있는 법적 근거를 주고 있다.

76) 개인정보보호법 제12조 및 제13조

의하여 국가 및 지방자치단체의 보건의료시책에 관한 내용의 공개를 청구할 권리를 가진다고 규정하고 있으며, 또한 모든 국민은 관계 법령이 정하는 바에 의하여 보건의료인 또는 보건의료기관에 대하여 자신의 보건의료와 관련한 기록 등의 열람이나 사본의 교부를 요청할 수 있으며 본인이 요청할 수 없는 경우에는 그 배우자·직계존비속 또는 배우자의 직계존속이, 그 배우자·직계존비속 및 배우자의 직계존속이 없거나 질병 기타 요청을 할 수 없는 부득이한 사유가 있는 경우에는 본인이 지정하는 대리인이 기록의 열람 등을 요청할 수 있다고 규정하고 있다.

그러나 의료법 제20조에서는 기록 열람 및 사본 교부에 대해 제한하고 있는데, 즉 의료법 제20조 제1항은 의료인 또는 의료기관 종사자는 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 환자에 관한 기록의 열람·사본교부 등 그 내용확인에 응하지 못하도록 하고 다만, 환자, 그 배우자, 그 직계존비속 또는 배우자의 직계존속(배우자·직계존비속 및 배우자의 직계존속이 없는 경우에는 환자가 지정하는 대리인)이 환자에 관한 기록의 열람·사본교부 등 그 내용확인을 요구한 때에는 환자의 치료목적상 불가피한 경우를 제외하고는 이에 응하도록 하고 있다.

제2항에서는 제1항의 규정에서 환자에 관한 기록의 열람·사본교부 등의 내용확인을 못하게 하고 있음에도 불구하고, 의료인은 동일한 환자의 진료 상 필요에 의하여 다른 의료기관에서 그 기록·임상소견서 및 치료경위서의 열람이나 사본의 송부를 요구한 때 또는 환자가 검사기록 및 방사선필름 등의 사본 교부를 요구한 때에는 이에 응하여야 한다고 규정하고 있다.

이러한 기록 열람 등에 관한 조항은 기본적으로 환자의 정보접근을 제한하고 예외적으로 접근을 허용하는 방식으로 기술되어 있어 적극적으로 정보주체의 정보 접근권을 보장하지 않고 있으며 환자에게 정보를 제공하

지 않을 수 있는 경우를 치료목적상 불가피한 경우로 모호하게 지정하여 의료정보에 대한 접근을 넓게 제한할 수 있다[77]는 문제가 있다.

정정청구권은 환자 측이 의료기관에서 관리되고 있는 정보가 부정확하거나 잘못되어 있다고 생각되는 경우에, 그에 관하여 정정을 청구하는 권리[78][79]이다. 의료정보 정정 청구권은 정보화시대에서 의료정보이용 상에 발생하는 의료정보의 훼손의 가능성이 높아진 환경에서 특히 중요하다. 미국의 HIPAA 프라이버시 규칙은 의료기관이나 의료인이 관리하고 있는 진료정보에 대하여 개인은 정보의 정정을 위한 서면요구와 정정내용을 뒷받침할 수 있는 자료를 제시하여 수록된 진료정보의 정정을 요구할 수 있도록 하고 있다. 의료정보의 정정을 요구받은 의료인이나 의료기관은 이러한 요구에 대하여 60일 이내에 타당한 조치를 취해야 한다[80]. 다만, 정정 요구된 내용을 당해 의료인이나 의료기관이 수집, 작성하지 않았을 경우, 정정 요구된 정보를 검토하기 위하여 접근할 수 없을 경우, 정정 요구된 정보가 정확하고 완전할 경우 등에는 의료기록의 정정을 거부할 수 있도록 하고 있다. 그러나 생각건대 정정청구권의 대상이 되는 의료정보는 의사의 전문적으로 판단하고 평가한 연구결과정보 등을 제외한 나머지 의무기록정보 및 객관적 사실에 국한된 의학정보에 한정될 것으로 판단된다.

삭제·차단청구권은 개인정보의 저장이나 보유가 허용되지 않거나 정보보유자의 직무수행에 더 이상 필요하지 않게 되는 경우에는 정보주체는 정보보유자에 대하여 자신에 관한 정보를 삭제할 것을 청구하거나 이용될 수 없도록 차단해 줄 것을 청구할 수 있는 권리[81]이다.

---

77) 윤경일, "정보화 시대의 환자진료정보 보호에 관한 법·제도적 고찰", 병원경영학회지 제8권 제2호, 119-120면
78) 개인정보보호법 제14조
79) 백윤철, 헌법상 의료정보에 대한 권리에 관한 연구, 헌법학 연구 제11권 제3호(2005.9), 346면
80) 백윤철, 미국의 의료정보와 의료정보보호, 의료정보의 정보화와 개인정보보호, 2006. 8. 16면
81) 권건보, "개인정보보호와 자기정보통제권", 경인문화사, 2005. 68면

5.1.1.3 이용 및 제공 통제권

이용 및 제공 통제권은 정보 침해 단계에서 발동되는 권리로서 침해 중단 청구권, 추가적 동의권, 개시 고지권 등[82]이 있다. 환자는 사전에 승인 등을 하지 않았음에도 불구하고, 정보가 개시된 경우에 사실을 고지해 받을 권리가 있다. HIPAA 규정에 따르면 환자에게 그러한 희망을 부여하면 과거 6년간으로 거슬러 올라가 개시가 이루어진 상황이나 상대방 등을 (1년에 1번) 무료로 입수할 수 있는 것으로 되어 있다[83]. 다만 이 규정의 의의는 사실상 부적절한 개시가 항상 감시되고 있다는 측면에서 사전에 부적절한 개시를 억제하고자 하는 것이라 할 수 있다. 그러나 이 개시기록의 고지가 필요한 범위는 치료 등과 관련되는 정보개시 및 환자가 사전에 승인을 한 치료 이외의 목적에서의 개시 등이 제외[84]되어 그 범위는 상당히 제한되어 있다.[85]

또한 정보주체는 자신에 관한 정보가 수집 당시 동의한 기간을 경과하여 이용되고 있거나 그 정보가 원래의 목적 이외의 용도로 처리되고 있는 경우 언제든지 그 이용이나 처리의 중단을 청구할 수 있다.

정보주체는 정보보유자에 대하여 자신에 관한 정보를 목적 외로 이용하거나 제3자에게 제공 또는 전달하는데 대한 동의권을 추가로 가진다. 정보주체가 정보의 보유자나 이용자로부터 새로운 사정에 대해 미리 통지받을 권리를 갖는 것은 이와 관련한 것이다.

---

82) 권건보, 위의 책, 70면

83) 백윤철, "헌법상 환자의 의료정보에 대한 권리에 관한 연구", 앞의 논문, 347-348면

84) Amendments to Final Rule, 67 Fed. Reg. 53181, 53244.

85) Standard for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82462, 82463(Dec. 28, 2000)(to be codified at 45 C. F. R., Pts. 160 and 164, 67 Fed. Reg. 53181(Aug. 14, 2002)(available at http://www.hhs.gov/ocr/hipaa/)(last visited on Step.1, 2002).

5.1.2 의료정보취급자의 의무

외부의 불법적인 침입으로 인한 정보의 유출을 방지하는 것 또한 개인의 의료정보보호를 위하여 중요하지만 내부의 불법적인 접근과 부실한 정보관리에 대한 대책 또한 중대한 문제로 대두하고 있다. 특히 의료기관에서 생성되는 의료정보에 대하여 현재는 각 의료기관별로 통일된 지침이 없어 기관 내부지침에 의해 접근하고 있는 실정이다. 그러나 각 의료기관별로 이러한 내부지침이 모두 다른데다 대부분 보건의료종사자들이 의료정보에 쉽게 접근할 수 있어 의료정보의 유출, 도난, 위조, 변조의 가능성이 항상 열려 있다고 할 수 있다. 따라서 의료정보취급자의 의료정보보호 관련 방안에 관한 사항을 법제도적으로 구체화하여 통일된 지침을 마련하는 것이 필요하다. 이러한 의료정보취급자의 의료정보보호 의무는 크게 의료정보의 안전보호와 비밀누설금지 의무인 사생활보호로 나누어진다.

<table>
<tr><th colspan="2">의료정보의 안전보호</th><th>의료정보의 사생활 보호</th></tr>
<tr><td>관리적
안전</td><td>내부 통제, 보안정책</td><td rowspan="4">-수집, 획득
-보유, 이용
-열람, 제공
의료정보취급자의
비밀유지 의무</td></tr>
<tr><td>기술적
안전</td><td>네트워크,
클라이언트, 서버
관리</td></tr>
<tr><td>물리적
안전</td><td>전산실 및 단말기 등
전산자료 관리</td></tr>
<tr><td>어플리케이션
안전</td><td>권한관리,
사용자관리,
공인인증서, 전자서명</td></tr>
</table>

표 12 의료정보취급자의 의무

5.1.2.1 개인의료정보의 안전보호

환자에 대한 모든 의료정보들이 컴퓨터를 통해 처리되는 과정에서 개인보건의료정보가 무단으로 노출, 누출 또는 위조, 변조, 손실, 삭제 등으로 침해를 당할 수 있기에 의료정보보호를 위하여 의료정보에 관한 보안 유지는 그 무엇보다 중요한 쟁점사항이라 할 수 있다.

이미 전자거래기본법 제2조[86]와 제4조[87] 및 전자서명법 제2조[88]를 비롯한 여러 법에서 전자문서의 문서성이 인정되어 왔으며, 보건의료분야에까지 전자문서의 효력을 확대할 필요성이 대두되어 개정 의료법은 전자의료기록에 대한 근거규정을 두어 그 문서성을 인정하기에 이르러 전자처방전과 전자의료기록 등이 법적 규율 내에서 이뤄지게 되었다. 현행 의료법은 전자의료기록에 대한 보호규정도 두고 있으며 이 규정들의 중요한 점은 전자처방전 및 전자의무기록의 비밀누설금지 또는 정보누출의 주체를 의료인에 제한하지 않고 모든 이로 확장하는 한편, 전자의무기록의 위·변조를 방지할 수 있는 장치와 백업장치 등을 갖추도록 하였다는 것이다.

이처럼 개인의료정보의 안전성을 확보하기 위한 보안유지 방법으로 기술적 안전장치 및 제도적 보안장치를 정하고 있기는 하나 컴퓨터 해커에 의한 진료기록에의 접근, 조작, 유포의 가능성은 여전히 존재하고 있으며 기타 정보통신 법률에 비해 구체적이지 못하여 실태 점검 등의 근거가 불명확하다. 환자 의료정보의 대량입력, 저장, 처리 등 의료정보화가 진행되면 될수록 보호되어야 할 의료정보 및 사생활의 영역이 점차 넓어지고 있

86) 전자문서의 정의 법률 제6614호 2002년 7월 1일 시행
87) 전자문서의 효력 법률 제6614호 2002년 7월 1일 시행
88) 전자서명법 제2조에서는 전자문서와 전자서명에 관한 정의, 동법 제3조에서는 전자서명의 효력 등에 관해 규정, 법률 제6585호, 2002년 4월 1일 시행

으므로 이에 충분히 대응할 수 있는 제도적 정비가 요구된다.

안전보호[89]는 정보시스템에서 전자적 형태의 정보를 처리, 저장, 전송하는 모든 단계에 걸쳐 고의 혹은 실수에 의한 불법적 노출, 변조 및 파괴 등 각종 위협으로부터 정보를 보호하여 아래와 같은 정보시스템의 기밀성, 무결성, 가용성을 보장하는 것[90]이다[91]. 첫째, 정보의 기밀성(Confidentiality), 인가 받지 않은 사람은 물리적·논리적으로 정보에 접근할 수 없어야 하며 접근하게 된 경우라도 정보를 해독할 수 없어야 한다. 둘째, 정보의 무결성(Integrity), 정보변경은 권한을 가진 사람이 정해진 절차에 따라서만 할 수 있어야 하며, 의도적이지 않은 정보 손실이나 자연 재해 등까지 고려해서 정보의 잘 보호되어야 한다. 셋째, 정보의 가용성(usability), 적절한 권한과 방법으로 접근한 사람은 언제나 정보를 사용할 수 있어야 하며, 정보를 관리하고 제공하는 방법에 있어 안정성을 유지해야 한다. 이 같은 원칙 하에 안전 보호의 대상을 기준으로 보안 절차를 나

89) 공공기관의개인정보보호에관한법률 제9조 (개인정보의 안전성확보등) 제1항에 의하면 공공기관의 장은 개인정보를 처리함에 있어서 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성확보에 필요한 조치를 강구하여야 한다. 또한 동법 제2항과 제3항은 공공기관의 장은 정보처리의 정확성 및 최신성을 확보하도록 노력하여야 하며 공공기관으로부터 개인정보의 처리를 위탁받은 자에 대하여도 제1항의 규정을 준용하고 있다.
개인정보보호지침 제17조(기술적 보호조치)에 의하면 서비스제공자 등은 컴퓨터를 이용하여 이용자의 개인정보를 취급하는 경우 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 백신 프로그램의 설치·운영 등 컴퓨터바이러스 방지 조치, 암호알고리즘 등의 이용을 통하여 개인정보를 안전하게 네트워크상에서 전송할 수 있는 보안 조치, 침입차단시스템 등 접근통제장치의 설치·운영, 기타 안전성 확보를 위하여 필요한 기술적 조치를 강구하여야 한다고 규정하고 있으며 동지침 제18조(관리적 보호조치) 제1항은 서비스제공자 등은 이용자의 개인정보에 대한 접근 및 관리에 필요한 절차 등을 마련하여 소속 직원으로 하여금 이를 숙지하고 준수하도록 하여야 한다고 정하고 제2항은 서비스제공자 등은 컴퓨터를 이용하여 이용자의 개인정보를 처리하는 경우에는 개인정보에 대한 접근권한을 가진 담당자를 지정하여 식별부호(ID) 및 비밀번호를 부여하여야 한다. 이 경우 서비스제공자 등은 해당 비밀번호를 정기적으로 갱신하여야 하며 제3항은 서비스제공자등은 인터넷 홈페이지를 통하여 회원가입 등 서비스이용계약 체결 또는 서비스제공을 위하여 이용자의 신용카드번호, 은행결제계좌 및 사용내역 등 대금결제에 관한 정보를 수집하거나 이용자에게 제공하는 경우 식별부호(ID) 및 비밀번호 확인, 전자서명의 사용 등 당해 이용자가 본인임을 확인하기 위하여 필요한 조치를 하여야 한다고 규정하고 있다.

90) 김용욱 외, Essential Elements of EHR system, 군자출판사, 2006.5, 114면

91) 대한의료정보학회, "보건의료정보학", 현문사, 1999, 233-274면

누어 보면 관리적 보안, 물리적 보안, 기술적 보안, 어플리케이션 보안의 네 가지[92]로 나누어진다.

가. 관리적 보안

관리적 보안은 인적·관리적·제도적 측면을 고려하여 개인정보 침해에 대비할 수 있도록 보안정책, 보안절차, 보안지침, 보안조직에 대한 지침 등을 결정하는 것이다.

나. 물리적 보안

물리적 보안은 출입통제와 작업감시, 전원대책, 선로 대책에 대한 관리이다

다. 기술적 보안

기술적 보안은 네트워크 보안[93], 클라이언트 보안, 서버보안, 통합관리[94]를 대상으로 한다. 기술적 보안에 관한 사항은 전산정보시스템에 관한 것으로 앞 장의 국내 의료 정보 현황에서 살펴 본 바와 같이 여러 병원들이 다양한 방법으로 그 보안에 심혈을 기울이고 있으며, 이는 IT 산업 기술의 발전으로 더 진보해 나갈 것으로 판단된다. 이 연구의 범위를 벗어나

92) 김용욱 외, Essential Elements of EHR system, 군자출판사, 2006.5, 115면
93) 네트워크에 연결된 컴퓨터 시스템의 운영 체제, 서버, 응용 프로그램 등의 취약점을 이용한 침입을 방지하기 위한 것이다. 일반적으로 네트워크 보안을 위해서 방화벽을 많이 사용했지만 요즘은 IPS, IDS 등 다른 여러 장비가 많이 사용되고 있다.
94) 일관성 있는 보안 관리를 위하여 인터넷침해사고 대응, 스팸메일 및 개인정보 보호활동 등을 관제하는 통합적으로 보안을 관리하는 것

다분히 기술적인 영역이므로 간략히 서술하는데 그치도록 하겠다.

라. 어플리케이션 보안

어플리케이션 보안은 주로 내부 사용자에 대해 기밀문서 및 내부 중요 문서의 외부 유출을 방지하기 위한 것이다. 권한관리, 사용자관리[95], 공인인증서 사용, 전자서명 등에 관한 것으로서 환자의 개인의료정보를 직접 담고 있는 전자의무기록과 연관성이 가장 큰 영역이라고 할 수 있다[96]. 환자의 의료정보에 대한 접근을 누구에게 어느 정도로 허용하는가에 대한 문제는 개인정보보호를 위한 첫 걸음으로서 이와 같은 접근권한의 관리에 대한 문제는 안전보호의 주요 쟁점이 되어왔다. 특히 의료정보화에 있어 무제한적으로 정보에의 접근이 가능해진 현시점에서 접근 권한의 제한은 내부로부터 이루어질 수 있는 의료정보침해를 방지하기위해 선행되어야 할 문제이다.

5.1.2.2 개인의료정보의 사생활 보호

형법 제317조에 따르면 의사, 한의사, 치과의사, 약제사, 약종상, 조산사, 변호사, 변리사, 공인회계사, 공증인, 대서업자나 그 직무상 보조자 또는 차등의 직에 있던 자가 그 업무처리 중 지득한 타인의 비밀을 누설한 때에는 3년 이하의 징역이나 금고, 10년 이하의 자격정지 또는 700만 원 이하의 벌금에 처한다고 있어 의사, 한의사, 치과의사, 약제사, 조산사 등의

95) 시스템 사용자에 대한 부서별 업무분장을 규정한다.
96) 김용욱, 앞의 책, 115면

의료인이 업무처리 중 지득한 남의 비밀을 누설하면 비밀누설죄로 처벌받게 된다[97].

이때, 비밀이라 함은 제한된 범위내의 사람들에게만 알려져 있는 사실로서 타인에게 전파되지 않음으로써 비밀주체에게 이익이 되는 사실을 말하며 비밀보장의 의사, 비밀을 보장할 필요성, 알려지지 않은 사항의 세 가지 요소로 구성되며 누설이라 함은 그 비밀을 모르는 제3자에게 고지하는 것을 말하며 구두이건 서면이건, 또 제3자가 1인이건 다수이건 불문하고 있다.

그러나 피해자의 승낙이 있는 경우, 법령상 비밀을 고지할 의무가 있는 경우(전염병 예방법 제4조, 형사 소송법 제112조, 제149조 등), 법익 균형의 원칙상 위법성이 조각되는 경우에 한해서는 비밀 누설이 합법적인 것으로 인정된다.

의료법 제19조 4에는 의료인은 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료, 조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못한다고 규정하고 있다[98]. 의료법 제20조 4에서 의료인은 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 환자에 관한 기록을 열람시키거나 그 기록의 내용 탐지에 응하지 못하도록 하였다. 그러나 제 1항의 규정에도 불구하고 의료인은 동일한 환자의 진료상 필요에 의하여 다른 의료기관에서 그 기록, 임상 소견서 및 치료 경위서의 열람이나 사본의 송부를 요구할 때 또는 환자가 검사 기록 및 방사선 필름 등의 차본 교부를 요구할 때에는 이에 응해야 한다는 예외를 인정하고 있다.

---

97) 이재상, 앞의 책, 223면
98) 한국의료법학회, "보건의료법학", 동림사, 2004, 264-267면

5.1.2.3 의료정보의 처리, 이용 및 제3자 제공 등

개인의료정보를 처리 및 이용 또는 제3자에게 제공하는 경우는 원칙적으로 환자의 의사에 따라야 한다. 이는 자기의 정보의 흐름을 적극적으로 통제하는 개인정보통제권의 핵심이기 때문이다. 다만 주지하였듯이 치료, 지불, 의료업무관리(TPO : **treat**ment, p**ay**men**t**, he**a**l**th** **car**e ope**rat**ion)에 의료정보가 사용되는 경우에는 환자의 동의 없이도 그 목적 범위 내에서 필요한 환자정보를 이용할 수 있다[99]고 할 것이다. 의무업무관리란 병원업무 및 의료의 질을 유지하고 개선하기 위한 활동이나 스탭의 교육 등을 포함한다. 그렇다면 환자명부 등재여부, 가족에 대한 개시, 연구이용, 공중위생 및 법집행 등 치료, 지불, 의료업무관리 이외의 개시의 경우 정보취급방침에 대하여 원칙과 예외를 구분하여 상세히 규정하고 할 필요가 있다.

99) 백윤철, "미국의 HIPAA법에 관한 연구", 앞의 책, 58면

5.2 의료정보보호 개선안

5.2.1 의료정보주체의 권리

5.2.1.1 수집통제권

수집통제권의 주요 내용인 수집동의권과 수집동의권의 전제조건인 설명청구권을 논함에 있어 개인의료정보 수집과 관련된 기준을 제시하는 것은 그 의미가 크다 할 것이다. 구체적으로 명확한 정보 수집 목적, 적절한 의료정보 수집 범위, 공정한 정보 수집 방법 등 세 부분으로 나누어 살펴보기로 한다.

가. 명확한 의료정보 수집 목적

1980년 '경제협력개발기구(OECD)'에서 발표한 「개인데이터의 국제유통과 프라이버시 보호에 관한 가이드라인」(OECD 가이드라인) 제9조는 "개인데이터의 수집목적은 늦어도 수집 시까지 명확화되어야 한다. 그 후의 이용은 수집목적의 실현 또는 수집목적과 부합되어야 하고 목적이 변경될 때마다 명확화될 수 있는 것으로 제한되어야 한다."고 정하고 있어 수집목적 제시가 개인정보보호와 관련한 중요 요소임을 나타낸다.

의료정보는 민감한 정보로서 침해 시 그 부작용이 현저하다 할 것임으로 그 침해 위험을 최소화하기 위해 환자로부터 특정 정보를 수집하게 될 경우 반드시 구체적인 수집목적을 밝혀야 한다. 즉, 수집하는 각각의 개인정보 항목에 대해 왜 수집하며, 어떤 목적으로 사용하게 될 것인가에 대해

이용자가 이해하기 쉬운 평이한 문장으로 상세하게 명시해야 한다.

나. 적절한 의료정보 수집의 범위

환자의 개인정보의 유출 위험은 의료정보 생성 시부터 발생되므로 반드시 필요한 최소한의 정보만을 수집하는 것이 유출 위험을 방지하는 최선의 방법이라고 할 수 있다. 이를 위해서는 반드시 필요한 정보에 대한 분석을 통한 정확한 내부 지침 마련이 선행하여야 할 필요가 있다.

그러나 현재는 보건의료기관들은 이러한 검토 없이 불필요한 정보까지 최대한 많이 수집하는 것을 관행화 하고 있고 보안 장치조차 제대로 마련하지 않고 있어 정보의 안전성이 위협되고 있는 상황이다.

「OECD 가이드라인」은 제 7조 에서 "개인데이터의 수집에는 제한을 두어야 한다."와 같이 수집제한의 원칙을 제시하고 있다. 다만, 국내에서는 현행 정보통신망이용촉진및정보보호등에관한법률[100]이 '서비스의 제공을 위하여 필요한 최소한의 정보'를 수집할 것을 명시하고 있지만 그 기준이 불분명하고 근거자료가 마련되지 않아 '최소한'이라는 문맥은 서비스제공자의 자의적인 해석에 의해 결정되고 있는 실정이다. 더욱이 의료정보의

100) 「정보통신망이용촉진및정보보호등에관한법률」(2001.7.1)은 개인정보의 수집 범위에 관하여 다음과 같이 규정하고 있다.
제23조 (개인정보의 수집의 제한 등) ①정보통신서비스제공자는 사상·신념·과거의 병력 등 개인의 권리·이익 및 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 이용자의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다. ②정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 당해 서비스의 제공을 거부하여서는 아니 된다. (시행일 2001 7 1)
개인정보보호지침」(2000 6 1)은 상기 법이 정하는 사항에 부연하여 다음 조항을 명시하고 있다.
제5조(수집의 구분) ①서비스제공자가 이용자의 개인정보를 수집하는 경우에는 기본적인 서비스 제공을 위하여 필요한 필수항목과 부가적인 서비스 제공을 위하여 필요한 선택항목으로 구분하여 이용자가 기입할 수 있도록 조치하여야 한다.
「정보통신망이용촉진및정보보호등에관한법률」(2001.7.1)의 제 23조 제 2항의 규정을 위반하여 개인정보를 수집하거나 서비스의 제공을 거부한 자는 500만 원 이하의 과태료에 처한다.

경우 적용이 어려운 규정이라 할 수 있으므로 별도의 지침이나 제도를 마련하여 세부적인 원칙을 제시할 필요가 있다. 특히 환자의 건강 정보 및 진단 정보와 같은 전문의료정보의 수집의 경우 그 전문성 및 의료행위의 성격으로 말미암아 구체적으로 요구되는 의료정보수집의 범위를 한정하는 것이 쉽지 않으나 환자 기초 정보 및 원무정보의 경우 일정한 한도에서 의료 행위의 내용에 따라 수집목적에 부합하는 정보만을 수집하도록 해야 할 것이다.

다. 의료정보 수집의 방법

수집방법은 의료정보 수집에 대한 정보주체자의 동의에 관한 사항을 말한다. 즉 정당한 방법으로 수집하였는가라는 문제는 곧 충분하고 적절한 설명을 제공하여 사전 동의를 받은 후에 정보를 수집하였는가의 문제이다.

「OECD 가이드라인」은 "어떠한 개인데이터도 합법적이고 공정한 절차에 의하고, 가능한 경우에는 데이터주체에게 알리거나 동의를 얻은 연후에 수집하여야 한다."고 공표함으로써 개인정보 수집방법의 중요성에 대해 언급하고 있다. 다른 법률에 의한 특별한 규정이 있는 경우를 제외한 모든 개인의료정보 수집절차는 반드시 합법적이고 정당한 방법 즉 적절한 절차에 따라 충분한 설명을 제공한 후 사전 동의를 받아 이루어져야 하며 그 외의 불법적인 의료정보 수집에 대한 강력한 통제가 필요하다.

다만 의식불명 등 법적으로 치료의무가 있는 긴급상태의 경우에는 사전 동의에 대한 예외적인 경우로서 사후 동의가 허용된다 할 것이다.

5.2.1.2 보유 통제권

정보주체에 대한 자기정보 접근권은 개인정보통제권의 핵심 내용으로서 환자의 정보접근권을 법률상 구체적인 권리로서 적극적으로 인정해야만 한다. HIPAA 또한 개인의 자기 의료정보에 대한 접근권을 보장하고 있으며[101] 다만, 정신치료 기록, 시민, 범죄, 행정 활동이나 처리에 사용하기 위해 컴파일된 정보 등은 대상에서 제외하고 있다. 조직은 이러한 요청을 수락할 의무가 있으며 요청 수령 후 30일 이내에 접근요청에 대하여 행동을 취하여야 한다.

현행 의료법 상 정보접근권이 20조의 기록 열람 및 사본 교부라는 형식으로 규정되어 있으나 치료목적상 불가피한 경우에는 이를 제한할 수 있다고 모호하게 규정되어 접근권이 사실상 넓게 제한될 여지가 있으므로 HIPAA처럼 구체적으로 정신과 치료 등으로 접근권이 제한[102]되는 범위를 한정할 필요가 있다. 또한 그 배우자, 직계존비속 또는 배우자의 직계존속이 환자에 대한 기록의 열람·사본교부 등 그 내용확인을 요구할 수 있도록 하고 있는 규정은 정보주체에 의사에 반한 정보에의 접근을 허용할 수 있으므로 본인 및 본인이 지정한 대리인만이 정보에 접근할 수 있도록 해야 할 것이다. 물론 미성년자 또는 심신지체 및 심신박약자 등 의사표현이 어렵다고 판단되는 근거가 있는 경우는 법정대리인[103]으로부터의 요청을 허용하되 반드시 사유를 문서화하여 남겨놓도록 하는 것이 바람직할 것이다.

정보화시대에서 의료정보 이용 시 발생하는 의료정보의 훼손 가능성이 높아진 환경에서 특히 정보의 오류가 야기하는 문제를 방지하기 위해서라

101) Final Rule, 65 Fed. Reg. 82462,82463.
102) Final Rule, 65 Fed. Reg. 82462
103) 김준호, 앞의 책, 289면, 285-290면

도 정보주체의 자기정보 수정 요청은 일정 부분 보장될 필요가 있다.

또한 본인의 요청에 의하지 않은 정보의 수정은 곧 정보의 훼손과 침해로 이어지므로 인가되지 않은 내·외부인의 수정 또는 의도하지 않았으나 실수에 의한 내부인의 수정 등 다양한 문제의 원인을 명확히 하기 위한 근거자료로써 정보의 수정이 있을 시에는 자동적으로 컴퓨터 파일에 기록을 남길 수 있도록 시스템을 운영하고 정보주체의 요청에 의한 수정일 경우에도 수정을 이행하는 자가 본인의 서명을 남기도록 해야 한다.

자신의 의료정보보호에 대하여 열람 및 정정청구권 등을 통하여 스스로 통제할 수 있도록 이들 권리를 실효성 있게 보장하기 위하여 행사 방법 등을 의료정보취급자가 환자에게 사전에 고지하거나 약관에 명시하도록 하고 고지사항 중의 일부는 구체적으로 지침을 마련해야 할 것이다. 어느 정도 기준을 명확히 해주는 것이 의료정보보호에 있어 효과적이기 때문이다.[104)]

5.2.1.3 이용 및 제공 통제권

기관이 수집한 정보주체의 정보를 제3자와 공유하였을 경우, 정보주체가 이에 대한 내역서[105)]조차 알지 못한다면 개인정보통제권을 보장받고 있다고 볼 수 없다. 의료정보의 가치가 높은 만큼 선의의 목적에 의해 정보가 활용될 수 있으나 그에 대한 정보주체의 알 권리 및 개인정보통제권이 충족되어야 하므로 제3자 제공 내역서 등을 받을 수 있는 개시 고지권을

104) 남효순, 앞의 책, 80면

105) HIPAA에 의하면 정보주체는 HIPAA의 적용을 받는 조직이나 제휴사를 대상으로 개인 보건의료정보의 공개 내역서를 요청할 권리가 있다. 다만, 치료, 의료비용 납입, 병원 운영, 국가 안보와 관련되었거나 사전에 본인 서명 승인을 받은 경우는 제외되며 내역 요청일로부터 최대 6년까지의 내역을 요청할 수 있다. 현행법에 의하면 모든 국민은 관계 법령이 정하는 바에 의하여 보건의료인 또는 보건의료기관에 대하여 자신의 보건의료와 관련한 기록 등의 열람이나 사본의 교부를 요청할 수 있다.

보장해 주어야 할 것이다.

또한 개인은 병원 등 보건의료기관을 대상으로 치료, 납입 또는 보건시스템 운영을 위한 보건의료정보의 사용 및 공개에 대한 제한을 요청할 권리를 가진다. 또한, 개인 건강관리나 의료비 지불에 관여된 사람에게 정보를 공개하거나 가족이나 친구 등에게 개인의 일반적인 상태나, 위치 또는 사망 정보를 공개하는 문제에 대해서도 제한을 요청할 수 있다.

5.2.2 의료정보취급자의 의무

5.2.2.1 개인의료정보의 안전보호

의료정보의 활용 및 보호에 관한 논의에 있어서는 법적 수단에 대한 논의뿐만 아니라 기술적 수단에 대한 논의도 중요한 고려사항이다 특히 전자자료 형태의 의료정보의 관리 및 처리 그리고 이에 대한 보호를 논함에 있어서는 보안 문제들이 중심적인 위치를 차지한다고 하여도 과언이 아니다. 따라서 정보통신 분야의 새로운 지식과 기술들을 의료 분야에 적용하여 의료정보의 활용의 효율성을 높이고 의료정보의 오·남용 가능성을 줄이는 방안을 모색해야 한다. 특히 의료 환경을 정확히 이해하고 가이드를 제시할만한 보안 전문가가 부족하여 안전보호를 위한 보안체계 및 전략 수립 등에 어려움이 많은 현 시점에서 의료정보의 안전성을 확보하기 위하여 단계별로 구체적인 기술적 안전장치 및 제도적 보안장치를 마련하는 것은 의미가 있다 하겠다.

가. 관리적 보안

의료정보취급자는 의료정보가 분실·도난·누출·변조·훼손 등이 되지 아니하도록 의료정보관리계획을 수립·이행해야 한다. 즉 천재지변, 파업, 사고 등 비상사태의 발생에 대비하여 의료정보시스템의 계속적 운영과 신속한 원상복구 등을 위한 비상대책을 수립, 운용해야 한다. 비상사태 이외에 평상시의 의료정보시스템 운용 및 의료정보보호를 위한 보안정책 및 보안 지침을 수립, 운용해야 함은 물론이다. 또한 의료정보취급자 및 관리자는 전산화된 의료정보의 유출, 파괴를 방지하기 위한 보호대책[106] 또한 수립, 운용하여야 한다.

또한 의료정보취급자는 암호 및 인증 시스템을 통한 의료정보관리를 원칙으로 하며 이에 적용되는 절차, 방법을 수립하여 안전하게 관리해야 한다. 더불어 의료정보누출의 우려가 있는 의료정보관리프로그램의 등록, 변경, 폐기 시의 절차를 수립, 운용한다.

의료정보취급자는 정기적으로 개인별 보안서약서를 작성케 하고 의료정보보호에 관한 정기적인 교육을 통하여 의료정보보호에 대한 중요성을 고취시키는 등 인적 관리에 대한 대책을 수립·운용해야 한다.

나. 기술적 보안

의료정보취급자는 정보시스템의 장애예방 및 시스템 성능의 최적화를 위하여 정기적으로 성능을 관리해야 한다. 이를 위하여 해킹 방지 대책 수립하고 운용하여야 하며 바이러스 감염 방지대책을 세워 감염에 대한 조속

106) 가령 .사용자계정 및 비밀번호를 개인별로 부여하고 관리한다든지, 환자정보의 조회, 출력 등을 통제하는 등 의료정보의 유출 및 파괴를 방지하기 위하여 최선의 노력을 다하여야 할 것이다.

한 대처를 하여야 한다. 또한 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 백신소프트웨어를 설치해야 할 것이다. 기술적 관리에는 통신망 및 네트워크와 보안공개용 웹서버에 관리대책도 또한 요구된다.

다. 물리적 보안

의료정보취급자 및 관리자는 의료정보전산실에 대한 화재, 수해 등의 재해와 외부의 위해방지대책 수립, 운용하여야 할 책임이 있다. 한편 의료정보전산실 출입자를 제한하고 통제하여야 하며, 의료정보를 다루는 단말기에 대한 보호조치 또한 이루어져야 할 것이다. 특히 전산의료정보 및 장비의 반·출입 통제하는 것은 물론이며 전산의료정보의 중요도에 따른 정기백업 실시 및 안전지역 소산, 기록 관리하는 것도 필요할 것이다.

라. 사용 관리

의료정보취급자가 의료정보를 이용 및 처리하기 위하여 접근할 때에는 서비스제공을 위하여 필요한 최소한의 인원에게만 부여하는 등 접근을 통제할 필요가 있다. 즉 의료정보에 접근하기 위하여 ID/패스워드 또는 전자인증서, 지문 등 생체 인식 등을 적용하여 인증된 사용자에게만 접근권한을 부여해야 한다. 또한 전보 또는 퇴직 등 인사이동이 발생하여 의료정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소해야 할 것이다.

또한 의료 정보는 구체적으로 나누어서 역할별로 사용 권한을 제한할

필요성이 있다. 즉 의료정보취급자가 적법한 요구를 하고 있는 정보에 대해서만 접근 및 수정, 조회, 삭제 등 이용 권한을 허용해야한다. 그러기 위해서 선행되어야 할 문제가 바로 환자 정보의 분류 및 역할별 업무의 범위를 한정하는 문제라고 할 수 있을 것이다. 환자의 정보가 구분되어야만 그 중요도를 구분하고 이에 대한 접근 및 이용에 있어서는 일정한 한계를 둘 수 있기 때문이다. 먼저 환자의 정보는 앞서 본 바와 같이 크게 환자기초정보, 전문의료정보, 원무정보로 분류할 수 있으며 다시 전문의료정보는 환자건강정보 및 진단정보로 나누어지고 원무정보는 처방전, 보험정보, 진단서로 분류될 수 있다.

역할별로 각 정보에 대한 접근을 제한하기 위하여는 역할별로 주어진 업무를 파악해야만 필요한 정보의 내용을 한정할 수 있을 것이다. 각각의 역할에 따른 세부적인 업무는 상당히 많지만 그 역할과 대표적인 업무만을 개괄하면 다음과 같다.

구 분	업무 내용
의사	진료(외래진료/병동진료), 상병 및 처방, 진료예약 및 퇴원처방 각종 제 증명 작성
간호사	환자 간호(외래/ 병동) 진료 지원 환자 간호 상담
간호 조무사	간호업무 보조 등
직원	환자관리- 입원 및 퇴원 수속, 제 증명관리, 고객 서비스/민원관리, 의무기록관리, 의료 통계 보험청구- 건강보험, 의료급여, 자보/산재 청구 등

표 13 역할별 업무 내용

위와 같은 정보의 종류와 역할별 업무의 범위를 바탕으로 접근 가능한 정보를 분류하면 담당의사는 원칙적으로 담당 환자에 대한 환자건강정보와 진단정보 즉 전문의료정보에의 접근이 가능하다. 물론 담당의사라 할지라도 근무 시간 내에 근무지를 이탈하지 않은 범위에서만 환자 정보의 접근을 허용해야할 필요가 있다. 간호사는 환자의 간호 및 진료 지원에 필요한 범위 내에서 환자기초정보에의 접근이 허용될 것이며 물론 담당 환자에 대한 근무 시간 내의 근무지 안에서의 접근만이 적법하게 인정될 것이다. 직원은 그 담당 업무에 따라 환자기초업무 및 보험 정보에 따른 접근이 허용될 수 있으며 다만 업무의 성질 상 진단서에 대한 접근이 부분적으로나마 허용될 여지가 있다. 만약 이러한 정보의 사용 권한에 대한 원칙적인 범위를 넘어 정보에 대해 접근·이용이 이루어졌다면 이것은 적법하지 못한 것으로 개인의 의료 정보에 대한 침해로 추정될 가능성이 있다. 다만 긴급한 필요에 의해 부득이한 경우 권한을 넘어 정보에 접근하는 경우, 또는 환자의 이익을 위해 필요한 경우는 예외가 허용된다고 할 수 있을 것이다.

5.2.2.2 개인의료정보의 사생활 보호

의료정보취급자는 개인의료정보의 보호를 위해 최선을 다할 의무[107]를 가진다. 따라서 의료정보취급자는 개인의 기밀 정보를 취급하는 자로서 보건의료정보보호 원칙에 입각하여 의료정보를 보호하기 위한 책임과 의무[108]를 충실히 이행해야할 것이다. 뿐만 아니라 보건의료정보화로 인해 의료정보의 수집·취급·관리 등을 위탁하는 경우, 위탁 처리되는 개인정보가 안전하게 관리될 수 있도록 선관주의의무를 져야할 것이다.

내부 정보취급자의 통제는 보건의료정보 관리의 안전성 보장을 위하여 반드시 해결되어야 할 문제로 양심과 윤리지침에 의한 자율규제가 대부분인 상황이나 정보침해의 상당부분이 내부 유출이며 이 경우 내부 취급자의 정보 접근성 등을 고려할 때 그 피해가 더욱 심각한 바, 명목상의 조항이 아닌 상세한 취급 가이드라인을 제시하고 지속적인 인식 제고 교육을 실시해야 할 필요가 있다.

또한 위반 시 벌칙 조항을 강화함으로써 비밀유지의 중요성을 인식하도록 조치해야 하며 이는 과거 보건의료정보를 취급하였던 자에 대해서도 동일하게 적용되어야 할 것이다.

개인정보 처리 위탁과 영업의 양수 등에 따른 의료정보취급자의 책임

107) 공공기관의개인정보보호에관한법률 제11조 (개인정보취급자의 의무)에 의하면 개인정보의 처리를 행하는 공공기관의 직원이나 직원이었던 자 또는 공공기관으로부터 개인정보의 처리업무를 위탁받아 그 업무에 종사하거나 종사하였던 자는 직무상 알게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위하여 사용하여서는 아니 된다고 정하고 있다.

108) 의료법 제19조는 의료인은 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료조산 또는 간호에 있어서 취득한 타인의 비밀을 누설하거나 발표하지 못한다고 하여 의료인에게 환자에 대한 비밀을 준수할 것을 규정하고 있다. 또한 동법 제67조는 이 규정에 위반한 경우 3년 이하의 징역 혹은 천만 원 이하의 벌금에 처하도록 하고 있다. 다만 이 경우에는 고소가 있어야만 공소를 제기할 수 있다. 형법 제317조 제1항도 의사 등이 업무처리 중 취득한 타인의 비밀을 누설한 경우 업무상비밀누설죄로 처벌하도록 하고 있다.

을 강화하고 환자를 보호할 수 있도록 규정해야 한다. 의료정보취급자가 이용자의 개인정보를 다른 사람에게 수집·처리·관리하도록 위탁하는 경우에 그 사실을 해당 환자에게 고지하도록 하고 위탁받은 사람을 그 업무의 범위 내에서 의료정보취급자의 소속직원으로 보아서 위탁받은 사람의 개인정보보호침해행위에 대하여도 의료정보취급자가 책임을 지도록 규정[109]하는 것도 고려될 수 있을 것이다.

109) 이은영, 개인의료정보보호 법안

5.2.2.3 의료정보의 처리, 이용, 제3자 제공 등

개인의료정보의 제3자 제공[110] 등에 관하여 개인을 식별할 수 있는 정보와 식별 정보가 삭제된 상태의 정보 공개는 구분할 필요가 있으며 개인식별이 가능한 정보공개의 경우에는 정보주체의 동의여부를 그 조건으로 하는 것을 원칙으로 해야 할 것이다.

가. 환자명부[111]의 공개

HIPAA 프라이버시규칙은 환자에게 환자명부에 자신의 정보를 공개할 것인지에 대하여 결정할 수 있도록 그 의사를 물어볼 것을 의무지우고 있다. 환자 명부의 등재 여부 또한 원칙적으로 환자의 의사에 따라야 할 것이며 다만 예외적으로 환자의 의사를 알 수 없는 긴급 상황의 경우에 동의없이 등재하는 것이 허용될 것이다.

---

110) 공공기관의개인정보보호에관한법률 제10조 (처리정보의 이용 및 제공의 제한) 제1항 및 제2항에 의하면 보유기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니 되며 제1항의 규정에 불구하고 정보주체의 동의가 있거나, 정보주체에게 제공하는 경우, 다른 법률에서 정하는 소관업무를 수행하기 위하여 당해 처리정보를 이용할 상당한 이유가 있는 경우, 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, 법원의 재판업무수행을 위하여 필요한 경우, 그리고 기타 대통령령이 정하는 특별한 사유가 있는 경우에 해당하는 경우에는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있도록 하고 있다. 다만, 위에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다고 명시하고 있다.

111) 환자명부는 입원환자의 이름과 병실, 기본적인 상황설명으로 구성되어 있음

나. 환자의 가족 및 지인에 대한 정보 제공

기본적으로 환자의 가족 및 지인에게 환자의 건강상태에 대한 설명을 해도 될 것인지 또는 어느 정도로 정보를 공개해야 할 것인지에 대하여도 환자의 결정에 따라야 할 것이다. HIPAA 프라이버시규칙도 이 문제를 환자에게 일임하고 있다.

다. 치료 목적의 이용

일반적으로 환자의 의료정보의 이용과 개시는 정당한 목적범위 내에서 요구되는 필요 최소한의 것에 한한다. 그러나 치료 목적의 이용 및 개시는 담당 환자의 치료를 위한 관련성 있는 정보에 대하여 접근이 제한을 받지 않는다 할 것이다. 다만 HIPAA 프라이버시규칙은 <정신과 치료기록[112]>의 경우 기록자인 담당 정신과 의사이외에는 환자가 특별히 서면으로 동의를 한 경우에 한하여 접근을 허용하고 있다.

라. 교육 목적의 이용

의과대학의 학생이 교육활동의 일환으로 환자의 의료정보에 접근할 필요가 있는 경우 원칙적으로 환자의 동의는 요구되지 않는다고 할 것이다. HIPAA 프라이버시 규칙도 이러한 교육활동은 의료업무관리[113]에 속하는 것이기 때문에 접근을 허용하고 있다. 다만 교육 목적에 필요한 최저한의 정보만을 이용할 수 있을 것이며 수정 및 삭제 등에 관한 사용 권한은 인

112) 정신과 치료를 행하는 전문가의 카운슬링 중에 얻은 기록으로서 환자의 의무기록으로부터 분리되어 보존되어 있는 경우만이 보호받는다.
113) Treatment, Payment and Healthcare Operation의 경우 환자의 동의없이도 이용이 가능하다.

정되지 않는다.

마. 연구 목적의 이용

연구 목적을 위한 의료정보의 이용에 있어서는 IRB[114]의 승인 여부 및 개인 식별가능성에 따라 달리 다루어져야 한다. 먼저 IRB에 의해 연구 계획이 승인된 경우와 의료정보에서 식별자가 제거된 경우는 환자의 허가 없이 의료정보에 대한 이용이 가능하다. 물론 IRB의 승인을 얻은 연구라 하더라도 HIPAA 프라이버시 규칙은 환자의 허가 없이 접근할 수 있는 정보에 대해 일정한 기준을 정하고 있다. 이 외에 연구를 위하여 환자의 의료정보에 접근하기 위하여는 연구자가 환자로부터 동의를 얻어야만 한다. 다만 식별자가 제거된 개인 식별불가 정보[115]로 인정되기 위해 삭제되어야 할 정보가 무엇인지에 관하여는 연구가 필요할 것이다.

바. 의료기관 간의 정보 제공

의료기관 간의 의료정보 제공은 원칙적으로 환자의 치료를 목적으로 환자의 동의가 있는 경우에만 인정되어야 한다. 다만 응급환자 본인이 요청하지 못하여 의료정보 제공에 대하여 사전 동의가 어려운 경우에는 예외적으로 사후적인 통지가 허용된다 할 것이다.

---

114) IRB 등에 의한 사전 연구프로토콜 심사는 반드시 충분히 환자의 권리를 지키지 못했다는 비판이 있다. 그러나 IRB 심사를 거치는 것으로 인해 환자의 동의 자체는 불필요한 것으로 되었다. http"//www.hhs.gov/ocr/hipaa/privacy.himl

115) HIPAA 규정은 환자 개인을 식별할 수 있는 변수로 전화번호, 팩스번호, 전자우편주소, 사회안전번호, 의무기록번호, 피보험자번호, 구좌번호, 면허번호, 차량번호, 의장번호, 웹URL, 인터넷 IP 주소, 지문이나 음성인식 등 생물학적 인식정보, 인물사진 또는 개인인식이 가능한 기타 고유번호나 특성 및 코드로 정하고 있다.

사. 건강 보험에의 정보 제공

보험의 지불요청을 위한 보험자에 대한 정보제공의 경우 즉 국민건강보험법의 규정 및 의료급여법의 규정에 의해 국민건강보험공단 및 건강보험심사평가원 또는 급여비용심사기관에 정보를 제공하는 경우 등에는 특별히 환자의 허가를 받을 필요는 없다. 그러나 더 중요한 문제는 이들 기관이 보유하고 집적하고 있는 의료정보가 굉장히 방대하고 중요함에도 불구하고 기본적으로 의료정보를 다루는 국민건강보험공단이나 건강보험심사평가원[116]의 의료정보보호에 관하여 다만 "행정 기관의 장은 그 산하기관 및 단체의 정보화에 관하여 필요한 시책을 강구하여야 한다[117]"고만 규정하여 현재 그 정보의 누출로 인한 침해가 심각함에도 불구하고 구체적인 보호에 미흡하다는 점이다.

아. 사법 수사 기관에의 정보 제공

환자가 피해자인 경우 원칙적으로 의료정보 제공에 대해서는 환자의 동의에 의하여야 할 것이지만, 의사무능력 상태에 빠져 허가를 할 수 없는 경우 시각을 다투고 있는 상황에서 환자의 이익을 위하여 필요하다면 의료정보의 제공이 허용된다 할 것이다. HIPAA 프라이버시규칙에서도 환자가 범죄피해자로서 정보제공 허가를 할 수 없는 경우 환자 허가 없이 사법집행기관에 정보를 제공할 수 있도록 규정하고 있다.

또한 그 밖의 경우에는 수사기관이 법원의 영장을 발부받아 요청하는 경우에만 환자의 동의 없이 의료정보를 제공할 수 있다 할 것이다.

---

116) 건강보험심사평가원은 개인정보보호법에 근거하여 건강보험개인정보보호처리지침(2001.5.10 지침 제12호.)을 적용하고 있다.

117) 전자정부법 제52조

의료행위는 필연적으로 환자 개인에 대한 의료정보를 생산해 내며 그와 같은 의료정보는 환자에 대한 진료에 있어서 뿐만 아니라 의학연구에 있어서도 중요한 자료로서의 기능을 하므로 의료행위 및 의학에 있어서 의료정보의 활용 및 정보 제공은 필수 불가결하다. 이처럼 의료정보는 환자 진료를 위한 목적과 함께 의과학, 병원경영, 보건행정 등 학문적인 연구에도 중요한 기초자료이나 의료정보가 개인의 사생활에 대한 비밀스러운 정보를 담고 있기 때문에 이에 대한 보호도 함께 고려되어야 함은 주지의 사실이다. 의료정보의 활용과 오·남용을 규율할 수 있는 법적 장치들은 아직 미미한 상태이므로 이에 대한 시급한 입법 및 지침이 필요하다 하겠다.

제6장 건강정보보호 입법안의 고찰

최근 대형의료기관 및 공공 기관들을 중심으로 의료 부분의 정보화가 급속히 진행되어 감에 따라 의료정보의 침해에 대한 우려의 목소리 또한 적지 않았음은 주지의 사실이다. 이에 의료계 및 학계·시민 단체를 비롯한 사회 각계 각층에서 민감한 정보인 의료정보를 보호하기 위한 입법의 필요성이 주장되어 왔다. 이러한 시대적 요청에 따라 보건복지부와 윤호중 의원 등은 각기 환자의 알권리를 보장하고 건강정보를 보호하기 위한 건강정보보호입법안을 제출하였다. “건강정보보호 및 관리·운영에 관한 법률 제정안”과 “건강정보보호법안”이 바로 그것이다. 미국 등 선진국이 종합적이고 구체적인 입법 체계를 갖추고 의료정보 침해 사태에 대비하고 있는 것에 비하여 조금 늦은 감이 없지 않지만 의료법만으로 의료정보에 대한 충분한 보호가 이루어지지 못하고 있는 현 시점에서 국민적 요구에 부합하는 개인의료정보보호법을 제정하고자 하는 이러한 시도들은 매우 고무적인 일이라 할 것이다. 이에, 국민의 알권리 및 자기결정권과 개인정보통제권을 보다 충실히 보장하고 의료계 및 관련업계에 의료정보보호와 관련된 최소한의 지침을 제공하는, 더욱 개선된 “개인의료정보보호법”을 제시하기 위하여 앞서 살펴 본 법적 쟁점 및 개선안을 토대로 각 입법안의 장·단점을 비교·분석해 보고자 한다.

6.1 구성

6.1.1 건강정보보호법률안

국회 보건복지위원인 윤호중 의원을 비롯한 총 26명의 국회의원들이 공동으로 발의한 “건강정보보호법률안”은 국민의 건강정보를 안전하게 보호하기 위하여 필요한 사항을 규정하고, 이를 토대로 건강정보의 정보화를 촉진하기 위한 기반을 마련함으로써, 국민의 건강증진에 이바지함을 목적으로 한다. 이는 모두 6개의 장으로 구성되며 그 내용으로 제1장 총칙, 제2장 건강정보에 대한 권리 및 보호, 제3장 건강정보의 정보화 운영체계, 제4장 건강정보의 정보화, 제5장 건강정보보호진흥원, 제6장 벌칙을 규정하고 있다. 본 장에서는 입법안의 내용 중 개인의료정보 보호와 직접 관련이 있는 총칙, 건강정보에 대한 권리 및 보호, 벌칙 부분에 한정하여 이를 검토해 보고자 한다.

6.1.2 건강정보보호 및 관리·운영에 관한 법률안

“건강정보보호 및 관리·운영에 관한 법률”은 국민의 건강정보를 보호하고 이를 체계적으로 관리 운영할 수 있는 기반을 조성하기 위해 보건복지부 보건의료정보화사업추진단에서 2004년부터 입법을 추진하고 있는 법률안이다. 이는 총칙, 건강정보의 보호, 건강정보의 관리·운영, 건강정보보호진흥원, 벌칙 등 총 5개의 장으로 구성된다. “건강정보보호 및 관리·운영에 관한 법률”에 대한 고찰도 마찬가지로 의료정보보호와 직접 관련이 있는 총칙, 건강정보의 보호, 벌칙 부분에 한정하기로 한다.

6.2 총칙

6.2.1 정의

각 법률안은 “건강 정보”를 건강과 관련한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료라 규정하고, “건강기록”을 국민 개개인의 건강상태 및 건강에 관한 활동을 기록한 것이라 정의하고 있다. 물론 민감한 정보인 건강정보 또는 건강 기록의 범위를 넓게 한정함으로써 가능한 그 보호에 만전을 기하고자 하는 의도는 충분히 이해할 수 있다. 그러나 각 법률안은 “건강정보” 또는 “건강기록”의 수집주체 및 수집목적에 대하여 규정하지 않음으로써 의료인 뿐 아니라 누구든지 건강에 관하여 표현 또는 기록한 자료이기만 하다면 그 목적을 불문하고 이 법의 보호 대상이 되는 “건강 정보” 내지 “건강 기록”에 포함되어 이 법의 규제를 받는다는 문제점을 갖는다. 각 법률안의 보호 대상이 “보건의료정보”라면 보건의료기본법 제3조 제6호에 규정되어 있는 보건의료와 관련한 지식 또는 부호, 숫자, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료라고 규정해도 별 문제가 없을 것이다. 동법 제3조 제1호에서 “보건의료”란 국민의 건강을 보호 증진하기 위하여 국가 지방자치단체 보건의료기관 또는 보건의료인 등이 행하는 모든 활동이라고 정의되어 있기 때문이다. 그러나 “건강 정보” 또는 “건강 기록”의 경우 그 어느 법률에도 나와 있지 않은 새로운 법률 용어이기 때문에 수집주체 및 건강 정보·기록의 수집목적 등에 관한 구체적인 정의가 필요하다.

윤호중 의원 법률안	복지부 법률안
제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. 1. “건강정보” 라 함은 건강과 관련한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료를 말한다. 2. “건강기록” 이라 함은 국민 개개인의 건강상태 및 건강에 관한 활동을 기록한 것을 말한다. 3. “전자건강기록” 이라 함은「전자서명법」에 의한 전자서명 또는「전자정부구현을위한행정업무등의전자화촉진에관한법률」에 의한 행정전자서명이 기재된 건강기록을 말한다. 4. “건강기록생성기관” (이하 “생성기관”이라 한다) 이라 함은 보건의료 관계 법령이 정하는 기관으로서 의료기관, 약국(「약사법」제72조의12의 규정에 의한 한국희귀의약품센터를 포함한다), 보건기관(보건소, 보건의료원, 보건지소, 보건진료소를 포함한다. 이하 같다), 그 밖에 이 법 제11조에 의한 건강정보보호위원회의 심의를 거쳐 보건복지부령으로 정하는 기관을 말한다. 5. “건강기록취급기관” (이하 “취급기관”이라 한다) 이라 함은 보건의료 관계 법령이 정하는 기관으로서 생성기관의 정보를 제공받아 취급하는 기관으로서, 질병관리본부, 국민건강보험공단, 건강보험심사평가원, 그 밖에 이 법 제11조에 의한 건강정보보호위원회의 심의를 거쳐 보건복지부령으로 정하는 기관을 말한다.	**제2조(정의)** 이 법에서 사용하는 용어의 정의는 다음과 같다. 1. “건강정보” 라 함은 건강과 관련한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료를 말한다. 2. “건강기록” 이라 함은 국민 개개인의 건강상태 및 건강에 관한 활동을 기록한 것을 말한다. 3. “전자건강기록” 이라 함은「전자서명법」에 의한 전자서명이 기재된 건강기록을 말한다. 4. “건강기록생성기관” (이하 “생성기관”이라 한다) 이라 함은 보건의료 관계 법령이 정하는 바에 의한 의료기관, 약국(「약사법」제72조의12의 규정에 의한 한국희귀의약품센터를 포함한다), 보건기관(보건소, 보건의료원, 보건지소, 보건진료소를 포함한다. 이하 같다), 그 밖에 제11조에 의한 건강정보보호위원회의 심의를 거쳐 보건복지부령으로 정하는 기관을 말한다. 5. “건강기록취급기관” (이하“취급기관”이라 한다) 이라 함은 보건의료 관계 법령이 정하는 바에 의하여 생성기관의 정보를 제공받아 취급하는 기관으로서, 질병관리본부, 국민건강보험공단, 건강보험심사평가원, 그 밖에 제11조에 의한 건강정보보호위원회의 심의를 거쳐 보건복지부령으로 정하는 기관을 말한다.

6.2.2 다른 법률과의 관계

각 법률안은 각 4조와 3조에서 다른 법률에 건강정보보호에 관한 규정이 있는 경우, 해당 규정이 각 법률안에서 정한 것보다 건강정보를 더욱 엄격하게 보호하는 경우에 한하여 그 법이 정하는 바를 따른다고 규정하고 있다. 그러나 다른 법률의 규정에 의하여 건강정보의 제공이 요구되는 경우 각 법률안이 제8조에서 건강기록 제공의 예외조항이라고 규정하고 있는 7개의 법률 이외에는 “다른 법률에 의하여 제공하고 있던 사항 중 이 법 제11조에 의한 건강정보보호위원회의 심의를 거쳐 대통령령으로 정하는 경우”에만 그 제공을 허용하고 있다. 따라서 위의 4조와 3조의 규정대로 해석할 경우, 각 법률안이 허용하고 있는 7개의 예외적인 경우를 제외하고 다른 법률에 의한 건강정보제공은 원칙적으로 금지되고 따로이 건강정보보호위원회의 심의를 거쳐 대통령령으로 정한 경우에만 건강정보제공이 허용되게 된다. 그러나 구지 다른 법률의 규정에 의하여 건강정보의 제공을 허용하고 있음에도 불구하고 건강정보보호위원회의 심의를 거쳐 법률보다 하위 규정인 대통령령을 통해 그 제공을 규제해야할 이유가 없다. 이는 기존에 “법률”에 의한 경우만 건강 정보를 제공하도록 법률 상 두텁게 보호되던 것을 “대통령령”에 의한 경우에도 건강 정보를 제공하게 만들어 오히려 이 법에 의해 건강정보를 약하게 보호하는 모순을 낳게 된다. 따라서 다른 법률과의 관계를 고려하여 제8조 1항 8호는 ‘기타 관련 법률에 의한 경우’로 손질하여야 할 필요가 있다.

윤호중 의원 법률안	복지부 법률안
제4조(다른 법률과의 관계) 다른 법률에 건강정보보호에 관한 규정이 있는 경우, 해당 규정이 이 법에서 정한 것보다 건강정보를 더욱 엄격하게 보호하는 경우에 한하여 그 법이 정하는 바를 따른다.	**제3조(다른 법률과의 관계)** 다른 법률에 건강정보보호에 관한 규정이 있는 경우, 해당 규정이 이 법에서 정한 것보다 건강정보를 더욱 엄격하게 보호하는 경우에 한하여 그 법이 정하는 바를 따른다.
제8조(건강기록 제공의 예외조항과 보호조치) ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.	**제8조(건강기록 제공의 예외조항과 보호조치)** ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.
8. 다른 법률에 의하여 제공하고 있던 사항 중 이 법 제11조에 의한 건강정보보호위원회의 심의를 거쳐 대통령령으로 정하는 경우	8. 다른 법률에 의하여 제공하고 있던 사항 중 이 법 제11조에 의한 건강정보보호위원회의 심의를 거쳐 대통령령으로 정하는 경우

6.3 건강정보의 보호

6.3.1 의료정보주체의 권리

6.3.1.1 수집통제권

각 법률안은 “건강정보보호의 기본원칙”이라는 제목으로 수집통제권의 주요 내용이 되는 수집동의권과 수집동의권의 바탕이 되는 설명청구권에 대하여 규정하고 있다. 이는 OECD 권고에 나타나 있는 수집제한의 원칙, 목적명확화의 원칙을 구체화한 것이라고도 할 수 있다. 이 규정은 당초 입법안에는 없던 내용을 신설한 것으로 의료정보의 보호에 있어 가장 기초가 되는 내용으로서 너무나 당연한 내용이지만 반드시 규정되어야 하는 부분이다.

가. 적절한 의료정보 수집의 범위

각 법률안은 의료정보 수집의 범위를 “특정한 이용목적에 따라 필요한 범위 안에서 최소한”으로 규정하고 있다. 이러한 원칙을 선언하는 것은 필요한 최소한의 정보만을 수집하는 것이 정보의 유출을 방지하는 최선의 방법이라는 점에서 의미 있는 일이다. 그러나 관행처럼 의료기관들이 불필요한 정보를 수집하고 있는 현 시점에서는 다만 이러한 원칙을 선언하는 데 그치는 것이 아니라 정부가 필요한 정보에 대한 분석을 통하여 정확한 지침을 마련해 줄 필요가 있다. 이러한 작업은 건강정보보호라는 목적을 더욱 공고히 해 줄 뿐 아니라, 의료기관의 부담을 덜고 의료정보 보호에 대한 인식을 높이는 역할을 할 것이다.

나. 의료정보 수집의 방법

각 법률안은 3항과 4항을 통해 동의의 원칙을 선언하고 그 방법에 대

하여 규정하고 있다. 다만 이 규정이 사문화되지 않기 위해서는, 긴급 사태 등 사전에 동의를 얻을 수 없는 경우를 제외하고 모든 동의는 사전 동의가 원칙이라는 점을 분명히 하고, 하위 규정을 통하여 HIPPA 프라이버시규칙처럼 의료기관의 의료정보취급방침통지 내용 및 방법을 구체적으로 규정할 필요가 있다.

윤호중 의원 법률안	복지부 법률안
제5조(건강정보보호의 기본원칙) ① 개인은 본인의 건강정보 내용 및 이용내역에 대하여 알권리를 갖는다.	**제4조(건강정보보호의 기본원칙)** ① 개인은 본인의 건강정보 내용 및 이용내역에 대하여 알권리를 갖는다.
② 개인의 건강정보는 특정한 이용목적에 따라 필요한 범위 안에서 최소한으로 수집되어야 한다.	② 개인의 건강정보는 특정한 이용목적에 따라 필요한 범위 안에서 최소한으로 수집되어야 한다.
③ 개인은 본인의 건강정보 제공 및 수집·가공·이용에 대하여 동의를 통해 결정할 권리를 가진다.	③ 개인은 본인의 건강정보 제공 및 수집·가공·이용에 대하여 동의를 통해 결정할 권리를 가진다.
④ 제3항의 규정에 의한 동의는 다음 각호의 원칙에 따른다.	④ 제3항의 규정에 의한 동의는 다음 각호의 원칙에 따른다.
1. 건강정보의 제공 및 수집·가공·이용에 대한 동의를 얻고자 하는 자는 이용목적, 수집의 범위, 이용절차, 보유기간 및 파기등에 관한 구체적인 사항을 이해하기 쉬운 형식으로 동의대상자에게 제공하여야 하며, 동의철회를 위한 방법을 포함하여야 한다.	1. 건강정보의 제공 및 수집·가공·이용에 대한 동의를 얻고자 하는 자는 이용목적, 수집의 범위, 이용절차, 보유기간 및 파기 등에 관한 구체적인 사항을 이해하기 쉬운 형식으로 동의대상자에게 제공하여야 하며, 동의철회를 위한 방법을 포함하여야 한다.
2. 어떠한 이유에서든 동의대상자의 동의여부 또는 동의철회에 따른 불이익이나 손해가 없어야 한다.	2. 어떠한 이유에서든 동의대상자의 동의여부 또는 동의철회에 따른 불이익이나 손해가 없어야 한다.

6.3.1.2 보유 통제권

각 법률안은 보유 통제권의 내용이 되는 열람 청구권과 정정청구권을 규정하고 있다. 이는 의료법 상에서 소극적으로 인정되던 열람 청구권 및

정정청구권을 적극적으로 인정하였다는 점에서 의미가 있다. 특히, 환자의 배우자, 직계존비속 또는 배우자의 직계존속이 환자에 관한 기록의 열람·사본교부 등 그 내용확인을 요구한 경우 이에 응하도록 규정하고 있는 의료법상의 규정과 달리 열람 및 정정 청구권을 환자와 그 법정·지정 대리인에게 한정시킴으로써 환자의 보호에 더 충실하였다는 점에서 고무적이다. 다만 정정청구권의 대상이 되는 내용을 "건강기록 중 명백한 오류"라고 규정하고 있어 자의적 해석의 우려가 있으므로 명문상 한정적으로 열거하여 논란의 여지를 방지할 필요가 있다.

윤호중 의원 법률안	복지부 법률안
제6조(열람 및 정정청구권) ① 본인, 법정대리인 또는 본인이 지정한 대리인은 해당 생성기관에 본인의 건강기록 및 건강기록의 이용내역에 대하여 열람·사본교부를 요청할 수 있으며, 해당 생성기관은 이에 응하여야 한다. 다만, 정신과 상담기록 등과 같이 본인 및 본인과 타인과의 관계 등에 위해를 줄 수 있는 기록이 포함된 경우, 해당 기록에 대한 열람·사본교부를 거부할 수 있다.	**제5조(열람 및 정정청구권)** ① 본인, 법정대리인 또는 본인이 지정한 대리인은 해당 생성기관에 본인의 건강기록 및 건강기록의 이용내역에 대하여 열람·사본교부를 요청할 수 있으며, 해당 생성기관은 이에 응하여야 한다. 다만, 정신과 상담기록 등과 같이 본인 및 본인과 타인과의 관계 등에 위해를 줄 수 있는 기록이 포함된 경우, 해당 기록에 대한 열람·사본교부를 거부할 수 있다.
② 본인의 건강기록 중 명백한 오류가 있어 이를 정정하고자 하는 자 또는 대리인은 해당 생성기관에 오류에 대한 정정을 요청할 수 있다.	② 본인의 건강기록 중 명백한 오류가 있어 이를 정정하고자 하는 자 또는 대리인은 해당 생성기관에 오류에 대한 정정을 요청할 수 있다.
③ 생성기관에서 환자의 건강기록을 작성한 자는 해당 환자 이외의 자가 그 건강기록을 열람하게 될 때는 그 이용내역에 대하여 알권리를 갖는다.	③ 생성기관에서 환자의 건강기록을 작성한 자는 해당 환자 이외의 자가 그 건강기록을 열람하게 될 때는 그 이용내역에 대하여 알권리를 갖는다.
④ 제2항 내지 제4항의 규정에 따른 열람·사본교부의 절차 및 범위, 열람·사본교부의 거부범위 및 절차, 오류의 범위 및 정정 절차, 이용내역외 열람 등에 관한 세부적인 사항은 보건복지부령으로 정한다.	④ 제2항 내지 제4항의 규정에 따른 열람·사본교부의 절차 및 범위, 열람·사본교부의 거부범위 및 절차, 오류의 범위 및 정정 절차, 이용내역외 열람 등에 관한 세부적인 사항은 보건복지부령으로 정한다.

6.3.1.3 이용 및 제공 통제권

가. 동의 철회권

개인은 자신에 관한 정보를 목적 외로 이용하거나 동의한 기간을 경과하여 이용되는 경우는 물론 목적 내에서 이용되고 있는 경우에도 동의를 철회할 수 있다. 이는 자신의 정보의 흐름을 정보 주체의 의사에 의하도록 하는 개인정보통제권의 내용상 당연한 일이라 할 것이다. 각 법률안 모두 이 점을 분명히 하고 있다.

윤호중 의원 법률안	복지부 법률안
제9조(동의의 철회 등) ① 제7조의 규정에 의한 건강기록의 제공 및 수집·가공·이용에 동의한 자는 그 동의를 철회할 수 있다.	**제9조(동의의 철회 등)** ① 제7조의 규정에 의한 건강기록의 제공 및 수집·가공·이용에 동의한 자는 그 동의를 철회할 수 있다.
② 제1항의 규정에 의하여 동의 철회 의사를 표명한 경우, 해당 건강기록을 제공받거나 수집·가공·이용한 자는 이를 지체 없이 파기하여야 하며, 그 파기사실을 동의를 철회한 자 및 해당 건강기록을 제공한 기관에게 통지하여야 한다.	② 제1항의 규정에 의하여 동의 철회 의사를 표명한 경우, 해당 건강기록을 제공받거나 수집·가공·이용한 자는 이를 지체 없이 파기하여야 하며, 그 파기사실을 동의를 철회한 자 및 해당 건강기록을 제공한 기관에게 통지하여야 한다.
③ 제1항 및 제2항의 규정에 의한 동의철회 절차, 파기 및 통지 등에 관한 세부적인 사항은 보건복지부령으로 정한다.	③ 제1항 및 제2항의 규정에 의한 동의철회 절차, 파기 및 통지 등에 관한 세부적인 사항은 보건복지부령으로 정한다.

나. 손해배상청구권

각 법률안은 이 법의 규정을 위반함으로써 피해를 입혔을 경우, “건강정보의 보호 및 정보화 촉진에 관한 업무를 수행하는 자” 또는 “건강기록의 보호 및 관리·운영에 관한 업무를 수행하는 자”에게 손해를 배상할 것을 규정하고 있다. 헌법상의 기본권인 개인정보통제권 및 사생활 비밀유지권 등이 법률상 구체적 청구권화 되어 재판상의 권리로 기능하는 것이라 할 수 있다. 다만 내부적인 유출의 위험 뿐 아니라 외부의 해킹 위험 또한 병존하고 있는 정보화 시대에 손해배상책임을 업무와 관련 있는 자로 한정할 이유는 없다고 판단된다.

그 밖에 각 법률안은 단서를 통해 건강정보의 침해로 인한 손해배상소송에서 고의·과실의 입증 책임이 가해자에게 있음을 명문으로 분명히 하고 있다. 따라서 가해자가 고의 또는 과실이 없음을 입증하지 못할 경우 고의·과실은 추정된다. 의료정보침해 피해자를 강하게 보호하고 의료정보의 침해 사태를 사전에 방지하려는 강한 의지의 표현이라 할 것이다.

윤호중 의원 법률안	복지부 법률안
제35조(손해배상) 건강정보의 보호 및 정보화 촉진에 관한 업무를 수행하는 자는 이 법의 규정을 위반함으로써 피해를 입은 자가 있는 경우에는 해당 피해자에 대하여 손해배상의 책임을 진다. 다만, 고의 또는 과실이 없음을 입증한 경우에는 그러하지 아니한다.	**제27조(손해배상)** 건강기록의 보호 및 관리·운영에 관한 업무를 수행하는 자는 이 법의 규정을 위반함으로써 피해를 입은 자가 있는 경우에는 당해 피해자에 대하여 손해배상의 책임을 진다. 다만, 고의 또는 과실이 없음을 입증한 경우에는 그러하지 아니한다.

다. 개시고지권

앞서 살펴 본, 동의철회권 및 손해배상청구권[118] 등 이용·제공 통제권이 실제적으로 보장받기 위해서는 정보주체가 자신의 정보의 이용에 대한 내용을 제공받아야 한다. 각 법률안은 "열람 및 정정청구권"을 규정하고 있는 각 6조와 5조의 제1항에서 "건강기록의 이용내역"에 대하여 열람·사본 교부를 요청할 수 있도록 함으로써 이러한 내용을 분명히 하고 있다. 다만 건강기록의 이용내역을 요청할 수 있는 근거는 마련되어 있으나 현실적으로 그 이용내역의 열람·사본교부 절차 및 범위 등 세부적인 사항에 대하여 규정하지 않고 있다는 문제점이 있다. 4항을 통해 이에 대한 절차 및 범위 등 세부적인 사항도 보건복지부령으로 정하도록 함이 마땅할 것이다. 건강기록 이용내역의 개시고지권은 현실적으로 비용이나 인력 등 의료기관 입장에서 번거롭고 부담스런 업무로 여겨질 수 있으나, 이는 환자의 의료정보에 관한 권리를 실효적으로 보장하기 위해 빠져서는 안되는 사항이라고 할 것이므로 이를 실현하기 위한 구체적인 검토가 필요하다.

윤호중 의원 법률안	복지부 법률안
제6조(열람 및 정정청구권) ① 본인, 법정대리인 또는 본인이 지정한 대리인은 해당 생성기관에 본인의 건강기록 및 건강기록의 이용내역에 대하여 열람·사본교부를 요청할 수 있으며, 해당 생성기관은 이에 응하여야 한다.	**제5조(열람 및 정정청구권)** ① 본인, 법정대리인 또는 본인이 지정한 대리인은 해당 생성기관에 본인의 건강기록 및 건강기록의 이용내역에 대하여 열람·사본교부를 요청할 수 있으며, 해당 생성기관은 이에 응하여야 한다.
④ 제2항 내지 제4항의 규정에 따른 열람·사본교부의 절차 및 범위, 열람·사본교부의 거부범위 및 절차, 오류의 범위 및 정정 절차, 이용내역외 열람 등에 관한 세부적인 사항은 보건복지부령으로 정한다.	④ 제2항 내지 제4항의 규정에 따른 열람·사본교부의 절차 및 범위, 열람·사본교부의 거부범위 및 절차, 오류의 범위 및 정정 절차, 이용내역외 열람 등에 관한 세부적인 사항은 보건복지부령으로 정한다.

118) 김준호, 앞의 책, 1545-1576면

6.3.2 의료정보취급자의 의무

6.3.2.1 개인의료정보의 안전보호

각 법률안은 의료정보의 안전성을 확보하기 위한 보안유지 방법으로 "건강기록의 보호조치"라는 제목 이하에서 관리적·물리적·기술적 조치가 포함된 정부 차원의 보호지침을 고시하고 이에 따르도록 규정하고 있다. 그 동안 우리나라는 의료법상 전자의무기록의 위·변조를 방지할 수 있는 장치와 백업장치 등을 갖추도록 함으로써 의료정보의 안전성을 확보하기 위한 근거 규정이 없는 것은 아니었으나 기타 정보통신 법률에 비해 구체적이지 못하다는 비판을 받아 왔다. 따라서 본 조항은 안전보호를 위한 보안체계 및 전략 수립 등에 어려움이 많은 현 시점에서 정부 차원의 지침을 마련해 줌으로써 의료기관의 부담을 경감시키는 한편, 의료정보보호를 위한 기반을 공고히 하는 근거 규정이 될 것이라 기대된다.

그러나 사실상 일부 대형병원을 제외한 우리나라 대부분의 병원들은 정보화 수준이 아직 열악하고 정보보호에 대한 인식 또한 매우 낮은 실정이다. 이러한 현실 속에서 의료정보보호라는 목적을 달성하기 위해서는 인력·시설·운영 능력 등 일정 수준 이상의 비용이 요구되며, 이는 병원으로서는 부담이 되지 않을 수 없는 문제임에 틀림없다. 따라서 이러한 현실을 고려하지 않은 정부의 지나치게 이상론적인 강요는 오히려 의료정보보호는 물론 현재 진행되고 있는 정보화에도 역효과를 발생시킬 우려가 있다. 그러므로 정부는 진정한 의료정보보호를 위해서 이러한 현실을 고려하는 한편, 국민과 의료계 및 관련 업계 모두가 수긍할 수 있는 현실적인 보호조치를 강구해야만 할 것이다.

윤호중 의원 법률안	복지부 법률안
제14조(건강기록의 보호조치) ① 보건복지부장관은 건강기록의 분실, 도난, 누출, 변조 또는 훼손 등에 대처할 수 있도록 다음 각호의 조치가 포함된 건강기록 보호지침(이하 “보호지침”이라 한다)을 생성기관 및 취급기관의 정보화 수준 및 규모에 따라 정하여 고시하여야 하며, 생성기관 및 취급기관은 이를 준수하여야 한다.	**제14조(건강기록의 보호조치)** ① 보건복지부장관은 건강기록의 분실, 도난, 누출, 변조 또는 훼손 등에 대처할 수 있도록 다음 각호의 조치가 포함된 건강기록 보호지침(이하 “보호지침”이라 한다)을 생성기관 및 취급기관의 정보화 수준 및 규모에 따라 정하여 고시하여야 하며, 생성기관 및 취급기관은 이를 준수하여야 한다.
1. 보안정책, 정보접근관리, 보안사고대응절차 등 관리적 조치	1. 보안정책, 정보접근관리, 보안사고대응절차 등 관리적 조치
2. 시설접근통제, 단말기 보안, 장치 및 매체 통제 등 물리적 조치	2. 시설접근통제, 단말기 보안, 장치 및 매체 통제 등 물리적 조치
3. 접근통제, 무결성, 인증, 전송보안, 네트워크 통제 등 기술적 조치	3. 접근통제, 무결성, 인증, 전송보안, 네트워크 통제 등 기술적 조치
② 생성기관 및 취급기관은 해당 기관의 관계자들에게 건강기록의 보호를 위하여 필요한 교육을 실시하여야 한다.	② 생성기관 및 취급기관은 해당 기관의 관계자들에게 건강기록의 보호를 위하여 필요한 교육을 실시하여야 한다.
③ 보건복지부장관은 국민 개개인이 자신의 건강정보를 보호하기 위한 권리의 내용과 그 행사방법을 정확하게 인지할 수 있도록 생성기관 및 취급기관과 함께 국민에게 필요한 사항을 교육·홍보할 수 있다.	③ 보건복지부장관은 국민 개개인이 자신의 건강정보를 보호하기 위한 권리의 내용과 그 행사방법을 정확하게 인지할 수 있도록 생성기관 및 취급기관과 함께 국민에게 필요한 사항을 교육·홍보할 수 있다.
④ 제1항의 규정에 따른 보호지침의 수립 및 시행에 관한 사항은 보건복지부령으로 정한다.	④ 제1항의 규정에 따른 보호지침의 수립 및 시행에 관한 사항은 보건복지부령으로 정한다.
⑤ 보건복지부장관은 제1항의 규정에 따른 보호지침의 준수 및 제2항 내지 제4항의 규정에 따른 교육·홍보에 필요한 비용의 전부 또는 일부를 보조할 수 있다.	⑤ 보건복지부장관은 제1항의 규정에 따른 보호지침의 준수 및 제2항 내지 제4항의 규정에 따른 교육·홍보에 필요한 비용의 전부 또는 일부를 보조할 수 있다.

6.3.2.2 개인의료정보의 사생활 보호

각 법률안은 “비밀 유지 등”이라는 제목으로 의료인을 비롯하여 건강 정보를 다루는 업무를 수행하거나 수행하였던 자 모두에게 업무상 알게 된 개인의 건강기록을 누설하거나 도용하지 못하도록 규정하고 있다. 이는 의료법상 의료인에게만 부과되어지던 비밀 누설 금지 의무를 의료인 외의 내부 건강정보 취급자에게도 부과함으로써 그동안 문제점으로 지적되어 왔던 내부 정보취급자의 정보 유출 문제를 통제하고자 한 것이라 할 것이다. 다만 각 법률안 어디에도 “건강정보 보호 및 정보화 촉진에 관한 업무(건강정보의 보호 및 관리·운영에 관한 업무)”에 대한 정의가 되어 있지 않아 생각하기에 따라 너무 막연하고 자의적인 해석이 가능하여 의도와 달리 오히려 비밀유지의무 부과대상이 지나치게 축소되거나 확대될 우려가 있다. 따라서 “건강기록생성기관 혹은 건강기록취급기관에 종사하거나 종사하였던 자 또는 이들 기관으로부터 건강정보의 처리업무를 위탁받아 그 업무에 종사하거나 종사하였던 자”로 한정하여 규정할 필요가 있다. 또한 그동안 의료법상으로는 “의료·조산 또는 간호에 있어서 취득한 타인의 비밀”이 비밀 누설 금지 의무의 내용이었으나 각 법률안은 모두 “업무상 알게 된 건강기록”으로 그 범위를 축소시키는 듯한 인상을 준다. 각 법률안은 “건강기록”을 국민 개개인의 건강상태 및 건강에 관한 활동을 기록한 것으로 한정하고 있는데, 환자의 민감한 건강 정보의 내용을 담고 있기만 하다면, “건강기록”외의 “건강정보”도 비밀 유지의 이익이 존재하므로 구지 비밀의 내용을 “건강기록”에 한정시킬 필요는 없을 것이다.

윤호중 의원 법률안	복지부 법률안
제25조(비밀유지 등) 이 법에 의한 건강정보 보호 및 정보화 촉진에 관한 업무를 수행하는 자 또는 수행하였던 자는 업무상 알게 된 개인의 건강기록을 누설하거나 도용하여서는 아니 된다.	**제16조(비밀유지 등)** 이 법에 의한 건강정보의 보호 및 관리·운영에 관한 업무를 수행하는 자 또는 수행하였던 자는 업무상 알게 된 개인의 건강기록을 누설하거나 도용하여서는 아니 된다.

6.3.2.3 의료정보의 처리, 이용, 제3자 제공 등

각 법률안 의료정보의 처리, 이용 및 제3자 제공 등에 관하여 “건강기록 교류시 정보보호”, “수집·가공·이용에 대한 정보보호”, “건강기록 제공의 예외조항과 보호조치”라는 제목으로 규정하고 있다. 자세히 살펴보면 다음과 같다.

가. 수집·가공·이용에 대한 정보보호

각 법률안은 개인 식별이 가능한 건강기록의 수집·가공·이용 및 제공을 원칙적으로 금지함을 명문으로 규정하고 있다. 그러나 개인 식별이 가능한 정보는 정보 주체인 환자의 동의가 전제하지 않을 때 그 수집·가공·이용 및 제공이 금지되는 것이다. 제7조 1항 전문의 규정이 민감한 정보인 건강기록을 특별히 보호해야 한다는 강한 사명감에서 도출된 것이라는 점과 반면 식별이 불가능한 정보에 대한 이용 가능성을 열어 두었다는 점에서 입법 의도는 충분히 이해할만하다. 그러나 이 규정을 그대로 적용할 경우 환자의 결정에 의한 건강기록의 이용 및 제공도 제한하게 되는 결과 정보주체의 개인정보통제권에 관한 지나친 제한이 될 수 있다. 따라서 이 법률안의 규정에도 불구하고 정보 주체인 환자의 동의가 있는 경우 식별이 가능한 건강 기록 및 건강 정보에 대하여도 그 수집·가공·이용 및 제공이 가능함을 분명히 해야 한다.

윤호중 의원 법률안	복지부 법률안
제7조(수집 · 가공 · 이용에 대한 정보보호) ① 누구든지 개인식별이 가능한 건강기록을 수집 · 가공 · 이용하거나 제공하여서는 아니 된다.	**제7조(수집 · 가공 · 이용에 대한 정보보호)** ① 누구든지 개인식별이 가능한 건강기록을 수집 · 가공 · 이용하거나 제공하여서는 아니 된다.

나. 치료 및 교육 목적의 이용

각 법률안은 제7조 1항 전문의 규정에도 불구하고 생성기관으로 하여금 환자의 직접 진료 및 교육을 목적으로 하는 경우에는 그 수집·이용을 허가하고 있다. 그러나 의료정보 생성기관이 환자의 건강정보를 수집·이용해야 하는 경우는 비단 진료 및 교육에만 국한되지 않는다. HIPAA 프라이버시 규칙에서 규정하고 있듯이 **Treatment, Payment and Healthcare Operation**의 경우에는 환자의 동의 없이도 그 업무의 범위 내에서 개인 식별이 가능한 정보의 수집·이용이 가능하도록 규정할 필요가 있다. 뿐만 아니라 제7조 1항 전문은 정보보호의 내용을 "건강기록"에만 한정하고 있어 건강정보 보호에 미흡하며, 후문은 수집·이용의 대상을 규정하지 않아 "건강기록"을 수집·이용할 수 있는 것인지 "건강 정보"를 수집·이용할 수 있는 것이지 명확하지 못하다는 문제가 있다.

윤호중 의원 법률안	복지부 법률안
제7조(수집·가공·이용에 대한 정보보호) ① 누구든지 개인식별이 가능한 건강기록을 수집·가공·이용하거나 제공하여서는 아니 된다. 다만, 생성기관은 해당 개인의 직접적인 진료를 목적으로 하는 경우와 교육법에 따른 교육과정에 따라 해당 개인의 진료와 관련한 교육을 목적으로 하는 경우에 한하여 수집·이용할 수 있다.	**제7조(수집·가공·이용에 대한 정보보호)** ① 누구든지 개인식별이 가능한 건강기록을 수집·가공·이용하거나 제공하여서는 아니 된다. 다만, 생성기관은 해당 개인의 직접적인 진료를 목적으로 하는 경우와 교육법에 따른 교육과정에 따라 해당 개인의 진료와 관련한 교육을 목적으로 하는 경우에 한하여 수집·이용할 수 있다.
⑥ 제1항 내지 제5항의 규정에 따른 개인식별정보의 범위, 생성기관의 수집 및 이용범위, 동의절차, 고지항목, 보호조치 및 파기절차 등에 관한 세부적인 사항은 보건복지부령으로 정한다.	⑥ 제1항 내지 제5항의 규정에 따른 개인식별정보의 범위, 생성기관의 수집 및 이용범위, 동의절차, 고지항목, 보호조치 및 파기절차 등에 관한 세부적인 사항은 보건복지부령으로 정한다.

다. 연구 목적의 이용

각 법률안은 기본적으로 식별 가능 건강기록을 통계·연구 목적으로 수집·가공·이용하고자 할 경우 본인 및 건강기록을 보유하고 있는 해당 생성기관의 사전 동의를 얻을 것을 요구하고 있다. 이는 식별가능 건강기록의 이용에 있어 본인과 생성기관 양자 모두의 동의를 요구함으로써 IRB의 승인만 있어도 의료정보의 이용이 가능한 HIPAA 프라이버시규칙보다 더 강한 보호를 취하고 있다고 할 수 있다. 그리고 그동안 제한 없이 이루어져 왔던 취급기관의 통계·연구 목적의 식별가능 건강기록에 대한 제공을 제7조 2항 후문을 통해 명문상 금지시킨 것은 상당히 고무적인 일이라 할 것이다. 그 밖에 각 법률안은 식별자가 제거된 건강기록의 경우에도 통계·연구목적으로 이들을 수집·가공·이용하려 할 경우 해당 생성기관 및 취급기관의 사전 동의를 얻도록 하고 있다. 식별자가 제거된 건강기록의 경우에도 물리적인 소유권은 이들 기관에게 있다할 것이므로 무분별한 사용을 막기 위해 필요한 규정이라 할 것이다.

윤호중 의원 법률안	복지부 법률안
제7조(수집·가공·이용에 대한 정보보호) ② 제1항의 규정에도 불구하고, 통계·연구목적으로 개인식별이 가능한 건강기록을 수집·가공·이용하고자 하는 자는 본인 및 건강기록을 보유하고 있는 해당 생성기관의 사전 동의를 얻어야 한다. 다만, 취급기관은 개인식별이 가능한 건강기록을 통계·연구목적으로 제공하여서는 아니 된다.	**제7조(수집·가공·이용에 대한 정보보호)** ② 제1항의 규정에도 불구하고, 통계·연구목적으로 개인식별이 가능한 건강기록을 수집·가공·이용하고자 하는 자는 본인 및 건강기록을 보유하고 있는 해당 생성기관의 사전 동의를 얻어야 한다. 다만, 취급기관은 개인식별이 가능한 건강기록을 통계·연구목적으로 제공하여서는 아니된다.
③ 통계·연구목적으로 개인식별정보가 제거된 건강기록을 수집·가공·이용하고자 하는 자는 해당 생성기관 또는 취급기관의 사전 동의를 얻어야 한다.	③ 통계·연구목적으로 개인식별정보가 제거된 건강기록을 수집·가공·이용하고자 하는 자는 해당 생성기관 또는 취급기관의 사전 동의를 얻어야 한다.

라. 의료기관 간의 정보 제공

각 법률안은 진료에 필요한 범위 내에서 본인, 법정·지정 대리인 또는 본인의 동의를 얻은 생성기관이 요청하는 경우 건강기록을 교류할 수 있도록 규정하고 있다. 즉 의료기관 간의 의료정보 제공은 원칙적으로 환자의 치료를 목적으로 환자의 동의가 있는 경우에만 인정되어야 한다는 원칙을 명문화 한 것이다. 다만 응급의료에 관한 법률 상 응급환자의 치료를 위하여 건강 기록이 필요함에도 불구하고[119] 본인이나 대리인의 사전 동의를 얻기 어려운 때[120]에는 사후적인 승인을 예외적으로 인정해 줘야 할 필요가 있다. 수정 전의 법률안은 명문으로 "응급의료에 관한 법률"에 의한 응급환자 본인이 직접 요청할 수 없는 상태인 경우, 당해 환자를 진료하고 있는 생성기관이 건강기록을 요청할 수 있도록 규정하고 후에 그 사실을 당해 환자에게 통지하도록 규정하고 있었음에도 수정 후에 이 부분을 삭제한 것으로 보인다. 그러나 현재 법률안의 내용은 이 법률안에 규정된 경우를 제외하고 다른 법률에 의한 경우에 건강기록을 제공하기 위해서는 따로 이 위원회의 심의를 거쳐 대통령령으로 정하도록 하고 있으므로 이 부분에 대한 검토가 필요하다.

윤호중 의원 법률안	복지부 법률안
제22조(건강기록의 교류) ① 생성기관은 다음 각 호의 어느 하나에 해당하는 자가 요청하는 경우 진료에 필요한 범위 내에서 다른 생성기관에 해당 건강기록을 열람시키거나, 사본을 교부할 수 있다.	**제6조(건강기록 교류시 정보보호)** ① 생성기관은 다음 각 호의 어느 하나에 해당하는 자가 요청하는 경우 진료에 필요한 범위 내에서 다른 생성기관에 해당 건강기록을 열람시키거나, 사본을 교부할 수 있다.
1. 본인 또는 법정 대리인	1. 본인 또는 법정 대리인
2. 본인이 지정한 대리인	2. 본인이 지정한 대리인
3. 본인의 동의를 얻은 생성기관	3. 본인의 동의를 얻은 생성기관

119) 응급의료에 관한 법률 제11조 (응급환자의 이송) ②의료기관의 장은 제1항의 규정에 의하여 응급환자를 이송하는 경우에는 응급환자의 안전한 이송에 필요한 의료기구 및 인력을 제공하여야 하며, 응급환자를 이송받는 의료기관에 진료에 필요한 의무기록을 제공하여야 한다.

120) 응급의료에 관한 법률 제9조 (응급의료의 설명·동의)
①응급의료종사자는 다음 각호의 1에 해당하는 경우를 제외하고는 응급환자에게 응급의료에 관하여 설명하고 그 동의를 얻어야 한다. 1. 응급환자가 의사결정능력이 없는 경우 2. 설명 및 동의절차로 인하여 응급의료가 지체되어 환자의 생명에 위험 또는 심신상의 중대한 장애를 초래하는 경우

마. 건강 보험에의 정보 제공

각 법률안은 본인의 동의없이 건강기록의 해당 부분을 제공할 수 있는 예외적인 경우로 “국민건강보험법”의 규정에 의해 국민건강보험공단 또는 건강보험심사평가원에 제공하는 경우와 “의료급여법”의 규정에 의해 급여비용심사기관에 제공하는 경우를 상정하고 있다. 무엇보다도 각 8조 3항과 4항에서 행정 기관의 장에게 일임하고 있던 국민건강보험공단 등의 건강정보 보호에 관한 사항을 직접 보건복지부령으로 정하도록 규정한 것은 바람직한 일이라 할 수 있다.

윤호중 의원 법률안	복지부 법률안
제8조(건강기록 제공의 예외조항과 보호조치) ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.	**제8조(건강기록 제공의 예외조항과 보호조치)** ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.
1.「국민건강보험법」제13조, 제43조 및 제56조의 규정에 따른 급여비용 심사·지급·사후관리 및 요양급여의 적정성 평가·가감지급 등을 위하여 국민건강보험공단 또는 건강보험심사평가원에 제공하는 경우	1.「국민건강보험법」제13조, 제43조 및 제56조의 규정에 따른 급여비용 심사·지급·사후관리 및 요양급여의 적정성 평가·가감지급 등을 위하여 국민건강보험공단 또는 건강보험심사평가원에 제공하는 경우
2.「의료급여법」제11조제2항의 규정에 따른 급여비용의 심사청구를 위하여 급여비용심사기관에 제공하는 경우	2.「의료급여법」제11조제2항의 규정에 따른 급여비용의 심사청구를 위하여 급여비용심사기관에 제공하는 경우
③ 제1항 및 제2항의 규정에 따라 건강기록을 제공받은 자는 해당 건강기록의 보호를 위하여 필요한 조치를 취하여야 하며, 목적 외의 용도로 이용하거나 제공하여서는 아니 된다.	③ 제1항 및 제2항의 규정에 따라 건강기록을 제공받은 자는 해당 건강기록의 보호를 위하여 필요한 조치를 취하여야 하며, 목적 외의 용도로 이용하거나 제공하여서는 아니 된다.
④ 제1항 내지 제3항의 규정에 따른 건강기록의 제공범위, 보호조치 등에 관한 세부적인 사항은 보건복지부령으로 정한다.	④ 제1항 내지 제3항의 규정에 따른 건강기록의 제공범위, 보호조치 등에 관한 세부적인 사항은 보건복지부령으로 정한다.

바. 사법 수사 기관에의 정보 제공

각 법률안은 수사기관이 법원의 영장을 발부받아 요청하는 경우에만 환자의 동의 없이 의료정보를 제공할 수 있다고 규정하고 있다. 이는 최근 행정 해석에서 경찰과 법원 등이 적법한 절차에 의하지 않고 환자의 의무기록을 요구할 경우 환자의 동의가 필요하다는 판단을 내린 것과 일맥상통하는 것으로서 수사 기관의 권력 남용으로부터 환자의 건강 정보를 보호하기 위한 합당한 조치로 여겨진다.

윤호중 의원 법률안	복지부 법률안
제8조(건강기록 제공의 예외조항과 보호조치) ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.	**제8조(건강기록 제공의 예외조항과 보호조치)** ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.
7.「형사소송법」제215조[121]의 규정에 따라 압수, 수색, 검증을 위하여 영장을 발부받아 요청하는 경우	7.「형사소송법」제215조의 규정에 따라 압수, 수색, 검증을 위하여 영장을 발부받아 요청하는 경우

사. 기타

각 법률은 전염병예방법, 혈액관리법, 후천성면역결핍증예방법, 결핵예방법 상의 신고 의무가 있는 경우에는 환자의 동의없이 건강기록을 제공할

121) 형사소송법 제215조 (압수, 수색, 검증)
①검사는 범죄수사에 필요한 때에는 지방법원판사에게 청구하여 발부받은 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.
②사법경찰관이 범죄수사에 필요한 때에는 검사에게 신청하여 검사의 청구로 지방법원판사가 발부한 영장에 의하여 압수, 수색 또는 검증을 할 수 있다.

수 있도록 규정하고 있다. 그러나 위의 4개의 법률 이외에도 모자보건법 제8조 3항과 4항의 규정에 의한 신고의무 및 아동복지법 제26조 2항 2호의 규정에 의한 아동학대신고의무 등에 의한 건강기록의 제공도 허용되어야 할 것이다.

윤호중 의원 법률안	복지부 법률안
제8조(건강기록 제공의 예외조항과 보호조치) ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.	**제8조(건강기록 제공의 예외조항과 보호조치)** ① 제7조제1항의 규정에도 불구하고 생성기관은 다음 각호의 어느 하나에 해당하는 경우에 관련 법률이 정하는 목적의 범위 안에서 본인의 동의 없이 건강기록의 해당부분을 발췌하여 제공할 수 있다.
3.「전염병예방법」제4조 내지 제6조 및 제21조의 규정에 따라 전염병 환자 및 예방접종 후 이상반응자 등이 발생하여 이를 보고 또는 신고하여야 하는 경우	3.「전염병예방법」제4조 내지 제6조 및 제21조의 규정에 따라 전염병 환자 및 예방접종 후 이상반응자 등이 발생하여 이를 보고 또는 신고하여야 하는 경우
4.「혈액관리법」제8조제2항 및 제10조제1항의 규정에 따라 부적격혈액을 발견하거나 특정수혈부작용이 발생하여 이를 보고 또는 신고하여야 하는 경우	4.「혈액관리법」제8조제2항 및 제10조제1항의 규정에 따라 부적격혈액을 발견하거나 특정수혈부작용이 발생하여 이를 보고 또는 신고하여야 하는 경우
5.「후천성면역결핍증예방법」제5조의 규정에 따라 감염자를 보고 또는 신고하여야 하는 경우	5.「후천성면역결핍증예방법」제5조의 규정에 따라 감염자를 보고 또는 신고하여야 하는 경우
6.「결핵예방법」제19조 및 제20조의 규정에 따라 결핵예방접종 및 결핵환자 등에 관한 사항을 보고 또는 신고하여야 하는 경우	6.「결핵예방법」제19조 및 제20조의 규정에 따라 결핵예방접종 및 결핵환자 등에 관한 사항을 보고 또는 신고하여야 하는 경우

6.3.3 기타

6.3.3.1 건강정보보호위원회

각 법률안은 생성기관 및 취급기관의 범위 및 건강기록 보호지침에 관한 사항 등을 심의하기 위하여 보건 복지부에 건강정보보호위원회를 두도록 규정하고, 그 산하에 보호위원회 사무국을 두고, 생성기관 및 취급기관이 기관정보보호위원회를 둘 수 있도록 하고 있다. 건강 정보 보호의 중요성 및 보안의 전문성을 고려할 때 각계의 전문가로 구성된 건강정보보호위원회를 설치하고 운영하는 것은 바람직한 일이라 할 것이다.

윤호중 의원 법률안	복지부 법률안
제11조(건강정보보호위원회) ① 건강정보보호에 관한 다음 각호의 사항을 심의하기 위하여 보건복지부에 건강정보보호위원회(이하 “보호위원회” 라 한다)를 둔다.	**제11조(건강정보보호위원회)** ① 건강정보보호에 관한 다음 각호의 사항을 심의하기 위하여 보건복지부에 건강정보보호위원회(이하 “보호위원회” 라 한다)를 둔다.
1. 제2조제4호의 생성기관 및 제5호의 취급기관 추가에 관한 사항	1. 제2조제4호의 생성기관 및 제5호의 취급기관 추가에 관한 사항
2. 제13조의 규정에 따른 기관건강정보보호위원회에 관한 사항	2. 제13조의 규정에 따른 기관건강정보보호위원회에 관한 사항
3. 제14조제1항의 규정에 따른 건강기록 보호지침에 관한 사항	3. 제14조제1항의 규정에 따른 건강기록 보호지침에 관한 사항
② 보호위원회는 의약계·시민단체(비영리민간단체지원법 제2조의 규정에 따른 비영리민간단체를 말한다. 이하 같다)·건강정보보호분야에 전문지식과 경험이 풍부한 학계 또는 민간전문가를 대표하는 자 중에서 보건복지부장관이 위촉하는 20인 이내의 자로 한다.	② 보호위원회는 의약계·시민단체(비영리민간단체지원법 제2조의 규정에 따른 비영리민간단체를 말한다. 이하 같다)·건강정보보호분야에 전문지식과 경험이 풍부한 학계 또는 민간전문가를 대표하는 자 중에서 보건복지부장관이 위촉하는 20인 이내의 자로 한다.
③ 보호위원회의 위원장은 위원 중에서 보건복지부장관이 임명하며, 제1항 제1호 내지 제3호에 관한 사항을 심의하기 위하여 분과위원회를 둘 수 있다.	③ 보호위원회의 위원장은 위원 중에서 보건복지부장관이 임명하며, 제1항 제1호 내지 제3호에 관한 사항을 심의하기 위하여 분과위원회를 둘 수 있다.
④ 보호위원회 및 분과위원회의 구성·운영 등에 관한 세부적인 사항은 보건복지부령으로 정한다.	④ 보호위원회 및 분과위원회의 구성·운영 등에 관한 세부적인 사항은 보건복지부령으로 정한다.

6.3.3.2 벌 칙

각 법률안은 이 법의 규정을 위반하거나 보호 의무를 준수하지 않은 자에게 과징금, 벌칙 및 과태료를 부과하는 등 행정벌과 형벌을 모두 규정하여 건강정보의 침해를 무겁게 처벌하고 있다. 일단 침해되면 원상복귀가 곤란한 민감한 건강 정보의 침해를 예방하기 위하여 사전에 위반자에게 강력한 처벌을 부과하는 한편 관리자에게는 무거운 책임을 지울 필요가 있다는 입법적 의도를 짐작할 수 있겠다. 특히 징벌적 손해배상제도를 도입하고 있지 않은 우리나라의 현실에 비추어, 건강정보를 이용하여 부당한 이득을 얻은 자에 대하여 그 경제적 이득의 30배 범위 안에서 과징금을 징수하도록 하는 것은 건강정보의 악의적인 상업적 이용을 방지하기 위해 필요한 일이다. 뿐만 아니라 각 법률안은 법인의 대표자 또는 법인이나 개인의 대리인, 사용인 그 밖에 종업원이 이 법의 위반하여 벌칙을 받게 되는 경우 법인이나 개인의 업무에 관하여 행위자 외의 그 법인 또는 개인에 대하여도 벌금형을 부과하고 있다. 정보보호를 위하여 자기의 지배범위 내에 있는 자가 위법행위를 하지 않도록 할 주의의무 및 감독의무가 있음을 명문으로 규정한 것이라 할 것이다.

윤호중 의원 법률안	복지부 법률안
제36조(과징금) 보건복지부장관은 이 법에 의한 규정을 위반하여 건강정보를 이용한 부당한 경제적 이득을 얻은 자에 대하여 그 경제적 이득의 30배의 금액을 초과하지 아니하는 범위 안에서 과징금을 부과할 수 있다.	**제28조(과징금)** 제4조 내지 제16조의 건강정보보호 규정을 위반하여 건강정보를 이용한 부당한 경제적 이득을 얻은 자는 그 경제적 이득의 30배의 범위 안에서 과징금을 징수할 수 있다.
제37조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년이하의 징역 또는 1천만원이하의 벌금에 처한다. 다만, 다음 각호의 규정을 위반한 자에 대한 공소는 고소가 있어야 한다.	**제29조(벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 5년이하의 징역 또는 3천만원이하의 벌금에 처한다. 단, 징역형과 벌금형을 병과 할 수 있다. 1. 제6조제1항의 규정을 위반하여 건

1. 제6조제1항의 규정을 위반한 자 2. 제7조제1항 내지 제4항의 규정을 위반하여 건강기록을 수집·가공·이용하거나 제공한 자 3. 제7조제5항의 규정에 의한 건강기록의 파기조치를 취하지 아니한 자 4. 제9조제1항의 규정에 의한 동의 철회 의사를 표명하였음에도 제9조제2항의 규정에 의한 파기조치를 취하지 아니한 자 5. 제22조제1항의 규정을 위반하여 건강기록을 열람하거나 사본을 교부받은 자 또는 제공한 자 6. 제25조의 규정에 의한 비밀유지 의무를 위반한 자	강기록을 열람하거나 사본을 교부받은 자 또는 제공한 자 2. 제7조제1항 내지 제3항의 규정을 위반하여 건강기록을 수집·가공·이용하거나 제공한 자 **제30조(벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 3년이하의 징역 또는 1천만원이하의 벌금에 처한다. 다만, 제1호의 규정을 위반한 자에 대한 공소는 고소가 있어야 한다. 1. 제5조제2항의 규정을 위반한 자 2. 제7조제5항의 규정에 의한 건강기록의 파기조치를 하지 아니한 자 3. 제9조제1항의 규정에 의한 동의 철회 의사를 표명하였음에도 제9조제2항의 규정에 의한 파기조치를 취하지 아니한 자 4. 제16조의 규정에 의한 비밀유지 의무를 위반한 자
제38조(과태료) ① 다음 각호의 어느 하나에 해당하는 자는 1천만원이하의 과태료에 처한다. 1. 제7조제5항 및 제9조제2항의 규정을 위반하여 건강기록의 파기사실을 통지하지 아니하거나, 허위로 통지한 자 2. 제14조제1항의 규정에 의한 보호지침을 준수하지 아니한 자 3. 제21조제2항의 규정을 위반하여 인증을 허위로 표시한 제품을 생산하거나 공급한 자 ② ~ ⑤ (생략)	**제31조(과태료)** ① 다음 각호의 어느 하나에 해당하는 자는 1천만원이하의 과태료에 처한다. 1. 제7조제5항 및 제9조제2항의 규정을 위반하여 건강기록의 파기사실을 통지하지 아니하거나, 허위로 통지한 자 2. 제14조제1항의 규정에 의한 보호지침을 준수하지 아니한 자 3. 제22조제2항의 규정을 위반하여 인증을 허위로 표시한 제품을 생산하거나 공급한 자 ② ~ ⑤ (생략)
제39조(양벌규정) 법인의 대표자 또는 법인이나 개인의 대리인, 사용인 그 밖에 종업원이 그 법인이나 개인의 업무에 관하여 제37조의 위반행위를 한 때에는 행위자를 처벌하는 외에 그 법인 또는 개인에 대하여도 동조의 벌금형을 과한다.	**제32조(양벌규정)** 법인의 대표자 또는 법인이나 개인의 대리인, 사용인 그 밖에 종업원이 그 법인이나 개인의 업무에 관하여 제29조 내지 제30조의 위반행위를 한 때에는 행위자를 처벌하는 외에 그 법인 또는 개인에 대하여도 동조의 벌금형을 과한다.

6.3.4 소결

이상에서 각 법률안의 건강정보보호와 관련된 주요 내용을 쟁점별로 나누어 살펴보았다. 각 법률안은 건강정보의 보호와 정보화라는 상호 의존적인 목적을 함께 달성하기 위한 것이기에 양자를 모두 규정하고 있으나 본 논문은 건강정보의 보호 부문에 한정하여 검토하였다. 각 법률안은 기본적으로 건강정보 보호와 관련한 원칙적인 사항들을 모두 규정하고 있다. 우선, 각 법률안은 “건강정보” 및 “건강기록”을 이 법의 보호 대상으로 정의하고 “건강정보생성기관” 및 “건강정보취급기관”을 규정함으로써 기존의 의료법보다 광범위하게 의료정보를 보호하려고 하고 있다. 그리고 각 법률안은 의료정보에 있어 개인정보통제권을 구체적으로 실현하기 위하여 반드시 필요한 내용이라 할 수 있는 환자의 권리인 동의수집권, 설명청구권, 열람 및 정정청구권, 기록개시권, 동의철회권, 손해배상청구권 등을 명문으로 규정하고 있으며, 의료정보를 관리·이용하는 건강정보생성기관 및 건강정보취급기관 등이 갖춰야 할 관리적, 기술적, 물리적인 보호 조치들에 관하여 지침을 마련하고 이에 따르도록 하고 있다. 또한 건강정보의 성격상 일단 침해되면 그 원상회복이 어렵다는 점을 감안하여 과징금, 형벌, 과태료 등 이 법의 위반 행위를 엄격히 처벌하고 사용자 및 법인 등에도 감독상의 책임을 물 수 있도록 양벌규정도 두고 있다는 것이 특징이라 할 수 있다. 기본적으로 정보화 시대를 맞이하여 국민의 의료정보를 보호해야 할 필요성과 당위성에 따라 건강정보 보호를 위한 지침을 마련해야 함은 앞서 누누이 강조하였던 바이며, 이제라도 건강정보 보호를 위한 법률을 제정하고자 하는 시도는 바람직한 일이라 판단된다. 또한 각 법률안들은 이러한 시대적 요청에 부응하는 다양한 내용을 담고 있다. 다만 각종 절차 및 고지·

동의 방법 등 세부적인 내용에 대해서 구체적으로 규정하지 아니하고 거의 대부분 하위법령에 위임하고 있어 각 법률안만으로는 실효성 있는 건강정보보호를 이루기 미흡한 점이 있다. 따라서 정부는 의료환경 및 의료정보보호 현황에 대한 면밀한 검토와 다양한 의견 수렴을 통하여 관련 의료 기관 단체 및 국민이 모두 수긍할 수 있는 구체적인 정책을 마련해야 할 것이다.

제7장 결 론

이상에서 헌법상의 기본권인 개인정보통제권을 바탕으로 도출되는 개인의료정보보호의 법적 의미 및 내용을 고찰함과 동시에 국·내외 의료정보보호 법제도와 현황을 살펴봄으로써 의료정보주체 및 의료정보취급자의 권리·의무 및 의료정보처리·이용과정에 따른 주요 쟁점사항을 검토하고 이를 토대로 현재 입법이 진행 중에 건강정보보호를 위한 법률안들을 내용을 분석해 보았다.

현대 정보통신 분야의 과학과 기술의 발전으로 말미암아 최근 의료부문에서도 공공기관 및 대형의료기관들을 중심으로 의료정보화가 활발히 추진 중이다. 이에 따라 개인의 의료정보가 대량으로 축적되어 데이터베이스화되고 정보에 대한 접근 및 이용이 간단해지게 되자 더불어 의료정보보호에 대한 관심도 증가하고 있다. 그러나 우리나라에서는 의료정보가 개인의 생명·신체와 직결된 사항이기 때문에 그 보호의 필요성이 매우 크다 할 것임에도 불구하고 의료정보 보호에 대한 종합적이고 구체적인 규정이나 의료정보보호와 보안에서 요구되는 내용을 충실히 포함하는 지침이 없는 상황이어서 이에 대한 합당한 검토 없이 극히 일부 공공기관 및 대형병원에서만 의료정보보호가 진행되고 있는 실정이다. 따라서 대부분의 병원의 경우 아주 기초적인 보안만이 이루어지고 있기 때문에 그 보호가 상당히 미흡하다 하겠다.

의료정보는 기본적으로 개인에 관한 정보이기 때문에 소극적 방어권으로서의 사생활의 비밀유지권의 보호대상이 되는 한편 공적 성격을 지니는 개인정보의 이용을 통한 효용을 창출케 하면서 적극적으로 자기정보 내지

개인정보에 대한 흐름을 감시 및 통제하는 개인정보통제권의 영역에서 보호를 받는다. 물론 개인정보통제권이 절대적으로 보호되는 권리가 아니기 때문에 정당한 공익상의 이유로 제한될 수 있는 권리임은 주지의 사실이다.

우리나라 의료법은 제19조는 의료인의 환자의 의료정보에 대한 비밀준수 의무를 규정하고, 개정 의료법 제18조의 2 제3항과 제21조의 2 제2항을 통해 전자의료기록 등에 대한 보호 규정도 두고 있어 의료정보보호에 대한 기본 근거가 없다고 할 수 없으나 이들 조항은 원칙적인 조항에 불과할 뿐 의료정보에 대한 정보주체의 권리 및 의료정보취급자의 의무에 대한 구체적 명시는 없어 헌법상의 기본권인 개인정보통제권의 내용을 충실히 반영하지 못하고 있다.

이에 비하여 국제적으로는 정보의 보호와 이용이라는 문제의 중요성을 일찍부터 인식하고 양자를 조화시키기 위하여 국제적인 정보보호지침 및 법제들을 입법화하여 활용하고 있다. 특히 OECD가이드라인의 개인정보보호 8 원칙 및 미국 HIPAA의 프라이버시규칙은 헌법상 기본권인 개인정보통제권의 내용 및 한계를 구체적으로 의료정보에 실현시키기 위한 모범이 된다 하겠다.

헌법상의 기본권인 개인정보통제권을 의료정보에 실현시키기 위한 내용으로서 개인정보통제권은 정보주체와 정보취급자에게 일정한 권리 및 의무를 부과한다. 그 권리·의무의 내용으로는 타인에게 알리고 싶지 않다고 생각하는 것이 정당한 일정한 사적인 의료정보에 대한 정보의 수집, 획득, 보유, 이용, 열람, 제공, 정보침해 각 단계에서의 통제권 및 이러한 권리를 실효적으로 확보하기 위한 의료정보의 열람청구권 및 정정청구권, 나아가 정보취급자에게 부과되는 정보수집의 목적 이외에 사용금지, 비밀유지 및

정보보안을 할 의무 등이 있다.

먼저, 환자의 의료정보에 대한 권리의 내용을 보장하기 위하여서는 수집 통제권, 보유 통제권 및 이용·제공 통제권을 OECD권고에 나타난 개인정보보호를 위한 8개 원칙 즉 수집제한의 원칙, 정보정확성의 원칙, 목적명확화의 원칙, 이용제한의 원칙, 안전보호의 원칙, 개인 참가의 원칙, 공개의 원칙, 책임의 원칙에 입각하여 입법적으로 구체화해 나가야 할 것이다. 구체적인 입법 체제가 없는 현 의료법체계로는 민감할 수밖에 없는 의료정보에 대한 권리가 복지부 등 행정기관의 유권 해석에 의존할 수밖에 없어 권리의 보장이 충분히 이뤄질 수 없기 때문이다. 따라서 헌법상의 추상적인 권리인 개인정보결정권의 내용 및 한계를 비례원칙의 파생 원칙이라 할 수 있는 OECD의 8개 원칙에 의거하여 구체적으로 규정할 필요가 있겠다.

의료정보취급자의 의무에 있어 관련된 문제는 비밀누설의 금지 및 보안 의무라 할 수 있다. 보안 의무의 경우 현재는 의료기관에서 생성되는 의료정보에 대하여 각 의료기관별로 통일된 지침이 없어 의료정보보호에 대하여 기관 내부지침에 의존하고 있는 실정이다. 대부분의 병원들이 보안체계 및 전략 수립에 대한 경험이 부족하고 그 기준이 정립되어 있지 않아 어려움을 호소하고 있는 현실 속에서 인적, 물리적, 관리적, 기술적 쟁점별로 정부 차원의 보안 가이드라인의 제시나 보안 기준이 마련되어야 의료정보화가 더욱 견실히 이뤄질 수 있을 것이다. 의료정보의 보호가 없는 의료정보화란 있을 수 없기 때문이다.

민감한 개인정보인 의료정보는 현대의 의술과 기술로도 정복하지 못한 미지의 영역에 속하는 정보로서, 그 자체가 무한한 정보원으로 효용성이 매우 높지만 개인의 입장에서는 엄중한 비밀이 보장되어야 하는 지극히 사적인 정보로서 그 수집 내지 보유만으로도 인격 침해의 가능성이 크며 한번 침해되면 원상회복이 어렵기 때문에 그 처리의 상황과 무관하게 특별히

강력한 보호가 필요하다. 그러나 보건의료분야의 정보화가 전개될수록 의료정보의 침해 가능성은 더욱 증가할 수밖에 없고 이러한 현실에서 양날의 검과 같은 성질을 가진 의료정보의 이용에 있어 사회제도적인 준비가 마련되지 않은 채 기술만 앞서가는 상황은 바람직하지 않다. 그런 의미에서 현재 입법이 추진되고 있는 건강정보보호를 위한 각각의 법률안은 이러한 시대적인 요청에 부응하기 위한 입법적 고려라 할 수 있을 것이다. 다만, 환자의 권리를 실효적으로 보장하고 의료계 및 관련업계에 의료정보보호를 위한 실질적인 지침을 제시하기에는 미흡한 점이 있는 것도 사실이다. 의료정보 보호를 위한 입법의 필요성을 모두가 인정하고 있음에도 불구하고 실질적으로 이에 대한 법률이 제정되지 못하고 있는 것은 바로 이러한 이유 때문이라 할 것이다. 의료의 질 보장과 환자의 권리보호를 위하여 정보를 유용하게 활용하는 동시에 불법적인 의료정보의 오·남용을 규율할 수 있는 법적 장치를 고안하기 위해서는, 좀 더 현실적이고 구체적인 연구를 통해 모두가 수긍할 수 있는 법안을 마련할 필요가 있다.

참고문헌

국내 단행본

권건보, “개인정보보호와 자기정보통제권”, 경인문화사, 2005

김용욱 외, “Essential Elements of EHR System" 군자출판사, 2006

김준호, “민법강의”, 법문사, 2006

김철수, “헌법학개론”, 박영사, 2006

남효순, “인터넷과 법률”, 법문사, 2005,

대한의료정보학회 (편저), “보건의료정보학”, 현문사, 1999

백윤철, “인터넷과 개인정보보호”, 신영사, 2002

이재상, “형법각론”, 박영사, 2000

전광석, “한국헌법론”, 법문사, 2006

한국의료법학회, “보건의료법학”, 동림사, 2004

허영, “한국헌법론”, 박영사, 2006

허영, “헌법이론과 헌법”, 박영사, 2006

국내 논문

강경근, “프라이버시 보호와 진료정보”, 헌법학연구 제10권 제2호, 2004

강경선, “사이버스페이스에서의 기본권”, 헌법학연구 제6권 제3호

김곤희, “우리나라 지역보건의료 EHR체계 구축 방안에 대한 연구”, 연세대 보건대학원 석사논문

김종철, “헌법적기본권으로서의개인정보통제권의재구성을위한시론”, 인터넷

법률4호2001.1.

백윤철, “미국의 HIPAA법에 관한 연구”, 인터넷법률 통권 제31호 2005.9

백윤철, “헌법상 환자의 의료정보에 대한 권리에 관한 연구”, 헌법학연구 제11권 제3호, 2005.9. 3

백윤철, “미국의 의료정보와 의료정보보호”, 의료정보의 정보화와 개인정보보호, 2006. 8.

백윤철, “헌법상 의료정보에 대한 권리에 관한 연구”, 헌법학 연구 제11권 제3호(2005.9)

연기영, “일본의 의료정보법제와 개인정보보호”, 중앙법학 제7집 제4호, 2005

윤경일, “정보화시대의 환자진료정보보호에 관한 법·제도적 고찰”, 병원경영학회지 제8권제2호

외국 문헌

A.Etzioni, "The Limits of Privacy", Basic Books, 1999,

Britten N et al, (1991). “Consultants’ and Patients’ View About Patient to their General Practice Records”, Journal of the Royal Society of Medicine. 84.

Convention for the protectoin of Individuals with regard to automatic processing of personal data, ETS No. 108

David Banisar & Simon Davies, “Global Trends in Privacy Protection : An international Survey of Privacy, Data Protection, and Surveillance Laws and Developments”, 18J. MARSHALL J.

Computer & Info. L. 1999

D.Flaherty, “Visions of Privacy: Past, Present, and Future”, University of Toronto Press, 1999

Géard Méeteau, “Cours de droit méical”, Les Etudes Hospitalièes, 2003.

Standards for privacy of individually identifiable health information. Final rule; correction of effective and compliance dates. Fed Regist (2001) 66(38):12434.

기 타

김정은, “진료정보공동활용 현황 및 추진방향 자료”, 2003

보건복지부, “지역보건의료분야 정보화 전략계획 수립 중간 보고서”, 2005

이유진, “정보보안 투자에 나선 병원, 그 현황과 과제”, 컴퓨터월드, 2005

이은영, “개인정보보호 법안”

윤호중 외, “건강정보보호 법안”

보건복지부 정보화추진사업단, “건강정보보호 및 관리·운영에 관한 법안”

한국보건산업진흥원, “국가보건의료 정보화계획(안)”, 2005

http://www.privacy.or.kr/guideline

http://www.hhs.gov/ocr/hipaa

http://www.hhs.gov/ocr/hipaa/privacy.himl

Abstract

A Study on the Protection Law for Individual Medical Information

Inkyoung Park

Dept. of Medical Law and Ethics

The Graduate School

Yonsei University

Individual medical information is a collection of all information that is gathered by patients and medical service providers in the long term and it includes the data gathered and analyzed by medical staff during the medical treatment. To cope with the changes of medical circumstance in information age, We need to utilize the medical information and hold it in common. But it has a danger to be violated easily through just collecting and holding information and it is to difficult to recover after the violation. So It is required to protect the individual medical information strongly.

Even though there are some regulations on the protection of medical information in medical law, they don't protect the medical information enough because we don't have a total and concrete law or guideline including contents on protection and security of medical information . Therefore we need a legal construction to protect the medical information properly and to control the current of own medical information, creating the effect by making use of the medical information on the basis of the right to control the individual information.

Based on the above-mentioned considerations, this study reviews

theoretically the constitutional meaning of individual information and protection of individual information, the legal meaning of medical information, and relation in the between medical information and the right to control the individual information to analyze the legal meanings and contents about the protection of medical information as individual information. All medical information should be protected in the basis on the right to control the individual information to seek both utilization and protection. this right to control the individual information imposes some legal rights and duty on patients and transactors.

Chapter 3 reviews the movements of the international legislation that remains to be solved in the legal · institutional sector to analyze the standards and rules as the ground of the protection of medical information.

Chapter 4 reviews the Korean current law and movement about the protection of medical information.

In Chapter 5, I summarize the issues discussed according to each patient and transactor and then I offer the improvement method on the ground of the above contents. In the first place, a patient has the right on the informed consent before collecting information to control the currents of information by own decision. And medical information should be collected by own informed consent in proper aim and bounds through the regal procedure. Second, Only a patient and a authorized agent have a right to access and a right to amend. Third, a patient has a right to suspend the violation, a additional right of informed consent and a right to an accounting of disclosure after violations. Fourth, medical information transactor must have the security systems including administrative, physical, technical and application security. fifth, transactor has basically a duty of care and both medical personnel and non-medical

personnel in the medical institution must keep the patient's privacy. Sixth, it is allowed to use the medical information without the patient's consent only in the case of treatment, payment and healthcare operation during processing, utilizing, and providing the medical information. Except treatment, payment and healthcare operation, we need a patient's consents to use and provide the medical information. However To prevent a variety of confusions, the rule and the exception should be prescribed to use and provide the medical information.

Chapter 6 reviews and analyzes a draft of proposed protection law for health information on the basis of the above-mentioned issues.

Chapter 7 is the conclusion of what has been discussed. Because the medical information has a lot of values as like a unlimited information source, the necessity of the using and sharing information would be increasing in information age and infringement possibility also must be increasing in proportion to it. Therefore, to improve the quality of medical service and to protect the right of patients, the appropriate improvement should be made by constructing the legal system, what we call, in harmony with the needs of the medical information age.

Key words : medical information, health information, the protection of medical information, HIPAA privacy rule, right to control the individual information