보건의료정보의 법적 보호와 열람·교부

정 용 엽*

I. 서 론

최근 병역문제와 관련하여 A시장 아들의 것이라고 주장하는 MRI(자기공

* 논문접수: 2012.4.24. * 심사개시: 2012.5.10. * 수정일: 2012.6.5. * 게재확정: 2012.6.8.
* 경희대학교의료원 QI팀장(의료품질관리), 경희법학연구소/경희대의료산업연구원 객원연구원, 서울사이버대학교 보건행정학과 강사, 법학박사
* 이 논문은 2012년 가을경 출간예정인 공동 저서 "보건의료정보학(가제)" 중 한 챕터(보건의료정보의 법률관계)의 초고를 수정 보완한 것입니다.

명영상진단) 촬영사진이 당사자나 가족이 아닌 특정인에 의해 공개되어 재촬영 대조하는 사태가 벌어지자 환자정보인 MRI 사진이 어떤 경로로 유출됐는지 사회적으로 큰 논란을 일으킨바 있다.[1] 또 국가기관인 B연구원이 유명 대학종합병원 등 6개 병원으로부터 환자 2,638명의 이름·전화번호·주소·주민등록번호·병록번호를 제공받아 이를 건강보험심사평가원 자료와 연계해서 근시교정술 관련 연구를 수행했다는 사실이 국정감사에서 지적되기도 했다.[2] 이는 의료기관이 환자를 진료한 후 진료기록(의무기록 차트) 형태로 만들어져 보관하는 환자 개인의 보건의료정보가 환자나 보호자 등 당사자가 아닌 제3자에 의해 불법적으로 유출된 사례에 해당한다.

또 대한의사협회는 600여 개 병·의원의 의료정보시스템을 관리·대행하고 있는 의료정보업체 A회사(모두 동의서를 받았다고 주장)가 '정당한 권한 없이' 또는 '허용된 접근권한을 넘어' 개별 병원의 의료정보 데이터베이스에 접근하여 전자처방전에 저장된 환자의 개인정보를 탐지하거나 누출한 것으로 파악하고 의료법 및 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반 혐의로 검찰에 고발했다. 이 사건의 경우 전국 병·의원의 34% 이상이 A회사의 의료정보시스템 프로그램을 사용하고 있기 때문에 전자의무기록 프로그램 데이터베이스에 저장된 환자 수는 가늠할 수 없을 정도로 많고 이러한 의료정보 관리대행 산업이 점차 확대되고 있는 추세인 점을 감안할 때 대단히 심각한 문제로 받아들여지고 있다.[3]

이처럼 근년에 들어와서 인터넷과 SNS(Social Network Service) 등 정보통신기술이 급속히 발달함에 따라 사회 각 분야에서 개인정보 유출문제가 사회적으로 심각한 화두로 대두됐고 우리나라도 그동안 시행해오던 관련 법률

---

1) 연합뉴스, "박원순 아들 세브란스병원서 MRI 촬영", 2. 22. 2012 (www. yonhapnews.co.kr/).
2) 국민일보 쿠키뉴스, "보건연, 6개 병원 2,000여 명 환자 정보 유출", 9. 29. 2011 (http://news.kukinews.com/).
3) 디지털데일리, "의협 vs 유비케어, 개인정보유출 논란 법정으로", 11. 8. 2010 (www.ddaily.co.kr/); 데일리메디, "의협, 유비케어 자료획득 자체가 위법", 11. 8. 2011 (www.dailymedi.com/).

들을 재정비하여 전면 대체입법한 개인정보보호법이 2011년 9월 30일부터 시행하기에 이르렀다. 이러한 맥락에서 의료계에서도 '민감한 정보'에 해당하는 환자의 개인정보 즉, 보건의료정보에 대해 그 의학적 활용이나 정보보호에 관한 문제가 본격적으로 논의되기 시작하여 보건복지부 주도로 의료기관 개인정보보호 가이드라인(500병상 이상 의료기관 대상)을 제정·공포하고 2010년 3월 15일부터 시행되었다. 그러나 이 제도의 시행 초기단계에 있는 현재 의료기관(병원)의 실무현장에서는 환자의 개인정보 보호를 위한 제도적·기술적 장치를 완벽하게 구축하지 못하고 있는 기관도 많으며, 특히 환자의 개인정보 보호의무를 가진 의사·간호사·일반직원 등 의료기관 종사자들의 경우 이에 대한 중요성을 정확하게 인식하고 관련 법규나 지침을 준수해서 병원업무를 수행해야 함에도 불구하고 아직까지 미흡한 실정인 것으로 파악된다.[4)]

이에 본고에서는 개인정보를 비롯한 보건의료정보의 법적인 개념과 국·내외의 관련 법제 현황에 대해 간략하게 살펴본 후, 보건의료정보의 침해에 대한 정보보호제도 및 그 열람에 따른 정보공개제도에 대하여 법제도적인 측면을 중심으로 총체적으로 검토해보고자 한다. 이를 통해 환자의 개인정보인 보건의료정보에 대한 법제도적인 장치와 보호의무 등에 관한 내용을 전반적으로 정리하고 그와 함께 문제점 및 개선방안을 제시함으로써 특히 보건의

---

4) 한편, 국내 5만 8천여 개 중소형 병·의원 중 상당수가 환자의 주민등록번호 등 개인정보 관리가 적절하게 이루어지지 않고 있고 진료정보에 대한 암호화 장치도 완벽하게 구축되지 못하고 있다. 특히 주민등록번호의 경우를 보면, 개인정보보호법에는 다른 법령에 근거가 있거나 본인동의가 있는 경우에만 요구할 수 있고, 의료법에는 진료과정에 주민등록번호가 필요하다면 이를 요구할 수 있도록 규정되어 있다. 그런데 병원 홈페이지 회원가입은 진료과정으로 간주되지 않으므로 주민등록번호 입력을 요구하면 아니 됨에도 불구하고 현재 중소형 병·의원의 70%가 이를 필수항목으로 요구하고 있어 문제다(전자신문, "중소병·의원들 개인정보 불감증 치료부터…", 3.19. 2012<www.etnews.com/> 참조); 이와 관련하여 진료과정에서도 개인정보보호법(일반법)보다 상위법인 의료법(특별법)에 따라 의료법시행규칙에서 강제하는 부분인 진료접수 시 주민등록번호·신체정보·질환정보 등 필수정보의 수집은 환자동의를 받지 않아도 되나 최소정보수집원칙에 의거하여 진료와 직접적인 관계가 없는 연락처(휴대폰번호)·이메일주소 등 그 밖의 개인정보에 대해서는 환자동의를 받아야 하고 이 경우에도 수집목적 외 이용 및 제3자 제공을 위해서는 별도 동의를 받아야 한다.

료정보를 취급하는 의료기관(병·의원) 및 그 종사자들이 이에 대해 정확히 숙지하고 실무현장에서 참고할 수 있도록 도움을 주고자 한다.

II. 보건의료정보의 개념

1. 보건의료정보의 법적 개념

가. 개인정보와 보건의료정보

보건의료정보(health & medical data)[5]는 보건의료행위 또는 의료행위 과정에서 만들어지는 개인정보의 특수한 형태이기 때문에 그 법적 개념에 대해서는 개인정보에서 찾아볼 수 있다. 우리나라 법제에서는 각 법률마다 약간 다르게 정의하고 있으나, 개인정보보호법·정보통신망법·전자서명법상의 정의를 종합해보면 대체로 개인정보(personal data)란 '살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는(식별 가능한: identifiable) 정보'라고 정의하고 있다. 여기에는 예시한 성명 등 이외에 부호·문자·음성·음향이나 생체특성 등에 관한 정보를 망라하고 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.[6] 이러한 개인정보의 개념에는 개인에 대한 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실 및 평가를 나타내는 일체의 정보가 포함된다.[7]

여기서 보건의료정보의 개념을 정의할 때에는 좁은 의미에서의 개념과 넓

---

5) '보건의료정보', '개인정보'의 영문표기에 대해서는 'medical information', 'personal information'이라고 하는 견해도 있으나(정부균, "환자 의료정보 보호의 문제", 『의료법학』, 제9권 제2호, 대한의료법학회, 2008.12, 제345면 참조), 본고에서는 OECD·UN·ILO 등 국제기구의 가이드라인 상의 영문표기법에 따라 'health & medical data', 'personal data'로 표기키로 한다.

6) 개인정보보호법 제2조 1호, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제2조 6호, 전자서명법 제2조 13호.

7) 권권보, 『개인정보보호와 자기정보통제권』, 경인문화사, 2005, 제17~20면 참조.

은 의미에서의 개념을 함께 살펴볼 필요가 있다. 먼저, 의료기관에서 환자의 개인정보를 의미하는 진료정보(협의의 보건의료정보)는 의사 등 의료종사자가 진료과정에서 환자에 대해 지득한 모든 정보를 말하며,[8] 이는 일반적으로 의료기관에서 진료기록 또는 의무기록(medical record) 형태로 기재된다. 그런데 판례에서는 '의료 내지 진료라는 특정 상황에서 환자의 상태와 치료경과 등 의료행위에 관한 사항과 소견'[9]이라고 정의하고 있으며, 실정법인 보건의료기본법 제3조 6호에서는 '보건의료와 관련한 지식 또는 부호·숫자·문자·음성·음향 및 영상 등으로 표현된 모든 종류의 자료'라고 정의하고 있다. 여기서 보건의료기본법 제3조 1호에 따르면 '보건의료'란 국민의 건강을 보호·증진하기 위해 국가, 지방자치단체, 보건의료기관, 보건의료인 등이 행하는 모든 활동을 말하는바, 광의의 보건의료정보는 의료기관에서 생성되는 진료정보 개념에 국가적 차원의 보건의료정책과 각종 보건의료사업 분야 등에서 생성 또는 유통되는 자료를 포괄하는 개념이라고 할 수 있다.[10] 여기서 협의의 보건의료정보와 광의의 보건의료정보의 개념상 차이를 살펴보면 그 작성주체가 전자는 의료기관과 그 종사자에 국한되는데 비해 후자는 국가·지방자치단체 및 각종 보건의료사업자와 그 종사자로 넓어진다는 점, 또 정보주체가 전자는 의료기관을 방문하는 환자에 국한되는데 비해 후자는 환자를 포함하여 일반 국민에까지 범위가 넓어진다는 점을 들 수 있다. 요컨대, 보건의료정보라 함은 보건의료와 관련하여 의료기관 및 기타 기관에서 생성되거나 유통되는 포괄적인 의미에서의 환자 및 일반 국민의 개인정보를 의미하는 것이다.[11]

---

8) 일본의사회, 『진료정보제공에 관한 지침 2-1(1)(번역문)』, 2002. 10. 22.

9) 대법원 1998.1.23. 선고 97도2124 판결.

10) 이경권, "환자 의료정보보호와 관련된 법적 쟁점", 『한국의료QA학회지』, 제15권 제2호, 한국의료QA학회, 제20면; 전영주, "의료정보와 개인정보보호", 『법학연구』, 제23집, 한국법학회, 2006.8, 제525면 참조.

11) 다만, 본고에서는 범위를 좁혀 의료기관에서 생성되는 환자의 진료정보 즉, 협의의 보건의료정보에 중점을 두고 의료 관련법과 개인정보보호법 상에서 어떻게 규정되고 보호되고 있는지에 대해 총체적으로 정리하고자 한다.

나. 보건의료정보의 종류

의료기관에서 의사 등 의료종사자에 의해 의무기록 형태로 작성되는 보건의료정보는 그 "생성(수집)→저장(축적) 및 보존(처리)→이용(유통)→폐기"라는 생명주기를 거치게 된다. 의료법 제22조에 따르면, 의료인 또는 의료기관 개설자는 진료기록부, 조산기록부, 간호기록부, 기타 진료에 관한 기록을 갖추고 의료행위에 관한 사항 및 의견을 상세히 기록·서명해야 하고 이를 법정기간 동안 보존해야 할 의무가 있다. 그리고 의료법 제23조는 이러한 의무기록을 전자서명이 기재된 전자문서, 즉 전자의무기록(electronic medical record: EMR) 형태로 작성·보존할 수 있도록 허용하고 있다. 또한 의료법 제18조 및 제19조에서는 의사·치과의사·한의사는 직접 진료한 환자에게 처방전을 작성하여 교부할 의무를 부여하고 있는데, 이때 처방전은 전자서명이 기재된 전자처방전 형태로 작성·발송할 수 있도록 허용하고 있다.

의무기록상 보건의료정보의 형식적인 종류는 의료법시행규칙 제14조~제15조에서 정하는 내용과 같다(아래 <표 2-1> 참조). 즉, 제14조의 의무기록 기재사항에서 열거하는 진료기록부·조산기록부·간호기록부와 제15조의 의무기록 보존연한에서 열거하는 처방전·수술기록·검사소견 기록·방사선사진 및 그 소견서·환자명부·진단서 등의 부본이 보건의료정보에 해당한다. 그밖에 병원행정 및 병원경영, 의학연구 및 의학교육, 국가보건의료정책 및 보건의료사업 분야 등의 업무수행과정에서 생성되는 보건의료정보는 별도로 정리될 수 있을 것이다.

이러한 보건의료정보의 종류에는 인쇄매체 형태의 의무기록(진료 차트) 및 처방전 이외에 이들을 전자적 장치를 이용하여 디지털화시킨 디지털보건의료정보(digital health & medical data)가 있으며, 의무기록과 전자의무기록이 대표적인 보건의료정보의 집적체라고 할 수 있다. 그런데 진료기록부 등 의무기록을 디지털화하는 방법에는 두 가지가 있다. 하나는 의료법 제23조에 따라 처음 생성단계에서부터 전자서명법에 따른 전자서명이 기재된 전자의

<표 2-1> 의무기록상 보건의료정보의 형식적 종류

의무기록의 기재사항 (의료법시행규칙 제14조)	의무기록의 보존연한 (의료법시행규칙 제15조)
1. 진료기록부 ⑴ 진료를 받은 자의 주소·성명·주민등록번호·병력(病歷) 및 가족력(家族歷) ⑵ 주된 증상, 진단 결과, 진료경과 및 예견 ⑶ 치료 내용(주사·투약·처치 등) ⑷ 진료 일시분(日時分)	① 진료기록부: 10년 ② 처방전: 2년 ③ 수술기록: 10년 ④ 검사소견 기록: 5년 ⑤ 방사선사진 및 그 소견서: 5년
2. 조산기록부 ⑴ 조산을 받은 자의 주소·성명·주민등록번호 ⑵ 생·사산별(生·死産別) 분만 횟수 ⑶ 임신 후의 경과와 그에 대한 소견 및 보건지도 요령 ⑷ 임신 중 의사에 의한 건강진단의 유무(결핵·성병에 관한 검사를 포함한다) ⑸ 분만장소 및 분만 연월일시분(年月日時分) ⑹ 분만의 경과 및 그 처치 ⑺ 산아(産兒) 수와 그 성별 및 생·사의 구별 ⑻ 산아와 태아부속물에 대한 소견 ⑼ 임부(姙婦)·해산부(解産婦)·산욕부(産褥婦) 또는 신생아에 대한 지도요령 ⑽ 산후의 의사의 건강진단의 필요성 유무	⑥ 조산기록부: 5년
3. 간호기록부 ⑴ 체온·맥박·호흡·혈압에 관한 사항 ⑵ 투약에 관한 사항 ⑶ 섭취 및 배설물에 관한 사항 ⑷ 처치와 간호에 관한 사항	⑦ 간호기록부: 5년
	⑧ 환자명부: 5년 ⑨ 진단서 등의 부본(진단서·사망진단서 및 시체검안서 등을 따로 구분하여 보존할 것): 3년

무기록(paperless chart) 형태로 작성하는 방법이며(EMR 단계), 여기에는 후술하는 OCS, LIS, PACS 등에서 생성된 보건의료정보도 포함된다. 다른 하나는 의료법시행규칙 제15조 제2항·제3항에 따라 인쇄매체 형태의 진료기록을 마이크로필름이나 광디스크 등으로 원본대로 보존하는 방법이며(CMR:

computerized medical record 단계)[12], 이 경우 필름촬영책임자가 필름표지에 촬영일시와 본인성명을 기재하고 서명 또는 날인하면 된다.

그런데 후자의 경우, 진료기록 원본과 스캐닝 필름의 동일성을 담보하는 방법으로 스캐닝작업을 수행한 필름촬영책임자(대개 병원에서는 의무기록실장이나 의료정보센터장 정도가 그러한 역할을 함)의 서명·날인방식을 규정하고 있는바, 하드웨어적인 측면에서 무결성(위·변조 방지)·진정성(작성자신분 증명)·부인봉쇄(사후 부인방지)와 객관성을 확보하는데 미흡한 점이 있다. 왜냐하면, 종이 의무기록을 마이크로필름이나 광디스크 형태로 변환시킨 것도 일종의 전자적 매체에 기록된 의무기록이고 전술한 <표 2-1>에서 정하고 있는 법상 기재사항이 기재되어 보존되어야 하는 것이기 때문에 의료법 제23조 제1항의 전자의무기록과 비교하여 하드웨어적인 작성방법에서 차이를 둘 이유가 없는 것이다. 따라서 이들 형태의 의무기록의 작성방법을 규정한 의료법시행규칙 제15조 제3항을 개정하여 전자의무기록에 준한 전자서명 방식으로 강화하는 것이 타당하다고 본다.

한편, 보건의료정보를 디지털화하는 일련의 과정을 보건의료정보화 내지 병원정보화(HIS: hospital information system: 병원종합경영정보시스템)라고 한다. 국내에서는 1978년 경희대학교의료원에서 최초로 병원행정전산화를 완성한 이래,[13] 오늘날 EDI, OCS, LIS, PACS, EMR 등의 방향으로 발전돼나가고 있다.[14] 그런데, 근년에 이르러 의료기관별 전자의무기록에 기

---

12) 정혜정·김남현, "보건의료의 정보화와 정보보호관리 체계", 『정보보호학회지』, 제19권 제1호, 한국정보보호학회, 2009.2, 제126~127면 참조.

13) 경희의료원(정용엽 외 5인 공저), 『경희의료원20년사』, 1992, 제178~180면 참조.

14) EDI(electronic data exchange) : 원무행정 분야에서 의료보험청구방식을 전산화하는 건강보험전자청구시스템, OCS(order communication system): 환자에게 발행하는 처방전을 전자적으로 전달하는 자동처방전달시스템, LIS(laboratory information system): 임상병리검사 등 각종 검사정보를 자동화하는 검사정보자동화시스템, PACS(picture archiving & communication system) : X-Ray·Sono·MRI·CT 등 각종 방사선촬영장치에서 발생되는 영상데이터를 디지털화해서 저장·검색·전송하는 영상정보저장전달시스템, EMR(electronic medical record): 환자의 진료기록을 전자적 형태로 기재하는 전자의무기록(정용엽, "u-헬스케어에 있어서 디지털의료정보의 법률적 보호", 『국제법무연구』, 제10호, 경희대학교 국제법무대학원, 2006. 2, 제18면; 정용엽, 『u-헬스 시대의 원격의료법』, 한국

술적 호환성을 갖추고 여러 기관에서 생성되는 개인의 건강관련기록을 디지털화 내지 네트워크화 하는 전자건강기록(EHR: electronic health record) 개념과 전통적 의료에 대비되는 새로운 의료형태로 Telemedicine(원격의료), u-헬스(ubiquitous healthcare), m-telemedicine(모바일원격진료) 등이 등장함에 따라 특히 디지털보건의료정보의 공동 활용 및 침해에 따른 보호문제가 쟁점으로 부상하고 있다.

2. 보건의료정보의 법적 성질

가. 보건의료정보의 기능

의료인은 대체로 병력청취와 이학적 검사지식을 체계적으로 기술하는 문제지향식 의무기록(POMR: Problem Oriental Medical Recording) 방식으로 의무기록을 작성한다. 또한 의무기록은 환자의 주관적 정보와 의료인(의료기관)의 객관적 정보 및 가치판단적 정보로 구성된다.[15] 판례에 따르면, 이렇게 보건의료정보가 기재된 의무기록은 환자에 대한 설명자료, 담당의사 및 다른 의료인의 진료 활용, 감독청에 대한 행정목적용 보고문서, 진료종료 후 또는 의료분쟁 발생 시 의료행위의 적정성 증명 및 환자의 권리의무 확정 증거자료로서의 기능을 가지고 있다.[16]

나. 보건의료정보의 특성 및 법적 성질

첫째, 보건의료정보는 의료전문가인 의료인과 환자 사이에서 이루어지는 진료행위라는 정보교환과정을 통해 생성된다는 특성을 가진다(전문성·협동성). 둘째, 보건의료정보는 의료기관 내에서 다수의 의료종사자에 의해 생성

학술정보(주), 2008. 5, 제370~375면 참조).

15) 이부하, "환자의 의료정보권", 『한양법학』, 제17집, 한양법학회, 2005, 제181~182면, 185~186면 참조.

16) 대법원 1998.1.23. 선고 97도2124 판결; 헌법재판소 2001.2.22. 선고 2000헌마604 결정.

되고 이들과 보험자 및 국가기관 등 사이에 필연적으로 공동 활용되는 특성을 가지고 있으며 이는 정보통신기술에 힘입은 보건의료정보의 컴퓨터화 내지 디지털화로 인해 한층 가속화되고 있다(유통성·유출성). 셋째, 보건의료정보는 개인의 건강이나 질병에 관한 정보로서 개인정보 가운데서도 '민감한 정보(sensitive data)'로 분류되어 강도 높게 보호된다(민감정보성).[17] 넷째, 보건의료정보는 의료인(의료기관)과 환자 간 의료계약을 시발점으로 진료과정을 통해 생성된다는 점에서 사적인 성질을 가지며 그 이후에는 직접적인 의료행위 이외에 국가보건의료정책과 각종 보건의료사업 분야에서도 광범위하게 이용될 수 있다는 점에서 공적인 성질을 띠고 있다(개인정보성·공익성).[18]

한편, 보건의료정보의 법적 성질을 살펴보면 보건의료정보는 인격권적 측면에서 보호되어야 하는 개인정보자기결정권에서 근거하는 것으로 일종의 기본권에 속한다. 그리고 일반적으로 정보주체는 환자이고 정보보유자는 의료기관이라고 보고 있다. 그런데, 재산권적 측면에서 보건의료정보의 법적 소유권(property: ownership)이 누구에게 있는가에 대해서는 ① 의료정보는 다른 어떤 정보보다 보호받아야 하는 것으로 의사는 환자 치료를 위해 환자정보의 일부를 사용할 수 있는 권한을 가지고 있을 뿐 진료기록부의 소유권은 환자에게 있다는 견해, ② 의사는 진료기록부 등에 기재할 수 있을 뿐 마음대로 수정할 수 없으므로 지적재산에 기초한 소유관계가 성립할 수 없다는 점에서 의사는 단순한 진료기록부 관리자라고 하는 견해, ③ 의사는 환자에 대한 객관적 사실과 의학적 판단을 함께 기록하므로 지적재산권에 유사한 소유관계가 성립한다고 보아 의무기록의 점유권 및 처분권한이 제한된 소유권은 의료기관에게 있으며 다만 의무기록에 대한 열람 및 사본교부권(의료

17) 개인정보보호법 제23조.

18) 길준규, "의료정보상 개인정보보호방안-독일법과 정보보호 법리를 중심으로", 『법과 정책연구』, 제6권 제1호, 한국법정책학회, 2006.6, 제123면; 백윤철, "우리나라에서 의료정보와 개인정보보호", 『헌법학연구』, 제11권 제1호, 한국헌법학회, 2005, 제417면 참조.

정보에 대한 접근권)은 환자에게 있다고 하는 견해 등이 대립되고 있다.[19] 이에 대해 미국에서는 진료기록(부)의 소유권은 의료기관에게 있고 그 물적 매체(진료기록부)에 내포되어 있는 의료정보의 소유권은 환자에게 있다고 보고 있으며, 후자에 근거하여 환자의 진료기록 접근권을 인정하고 있다(미국 의무기록 접근에 관한 법률, 1991). 요컨대, 환자의 보건의료정보는 의료인(의료기관)과 환자 사이의 협력관계로 이루어지는 진료과정에서 생성되는 환자의 개인정보를 바탕으로 의료인(의료기관)의 객관적인 분석자료와 전문지식 및 가치판단이 첨가되어 작성·보관되고 법률상 그 작성·보존의무가 의료인(의료기관)에게 부여되어 있는 한편 정보주체인 환자 본인에게는 법률상 그 열람 및 사본교부권이 부여되어 있다는 점에서 그 소유권은 의료기관에 있다는 견해가 타당하다고 본다.[20]

III. 국내·외 보건의료정보 법제

1. 외국의 보건의료정보 법제

일반 개인정보에 관한 국제적 규범으로는 OECD, UN, EU, ILO 등이 제정한 가이드라인이 각국의 일반 개인정보 법제에 영향을 미쳤으며,[21] 특히 보

---

19) 이백휴, "환자의 의무기록 관련 의료인의 법적 지위", 『의료법학』, 제11권 제2호, 대한의료법학회, 2010.12, 제312~313면 참조.

20) 전영주, "의료법상 의료정보 보호방안-의무기록 보호를 중심으로", 『법학연구』, 제28집, 2007.11, 제471~472면 참조.

21) OECD 개인데이터의 국제적 유통과 프라이버시 보호에 관한 가이드라인(OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980), UN 개인정보파일의 전산화에 관한 가이드라인(UN Guidelines Concerning Computerized Personal Data Files, 1990), EU 개인정보보호에 관한 유럽연합지침(The Protection of Individuals with regard to the Procession of Personal Data and on the Free Movement of such Data, 1995), ILO 근로자의 개인정보보호규약(ILO Code of Practice on the Protection of Worker's Personal Data, 1997); 특히 OECD는 개인정보보호 8원칙(수집제한원칙, 정보정확성원칙, 목적명확화원칙, 이용제한원칙, 안전보호원칙, 개인참가원칙, 공개원칙, 책임원칙)을 제시했다.

건의료정보와 관련하여 미국과 독일의 정보보호 법제를 간략히 살펴보면 아래와 같다.

⑴ 미국: 건강보험의 이전 및 책임에 관한 법률(HIPAA: Health Insurance Portability and Accountability Act, 1996) Ⅱ-F (Administrative Simplification) 및 그 시행규칙인 식별가능한 개인보건의료정보의 보호에 관한 표준(Standards for Privacy of Individually Identifiable Health Information, 2003: 일명 HIPAA 프라이버시규칙)에서 개인의료정보를 다루고 있다. 여기서는 규칙의 적용대상기관(의료보험자·의료제공자·의료정보전달기관), 보호되는 정보(개인식별 의료정보), 보호되지 않는 정보(개인익명화 정보), 의료정보의 이용과 제공 등을 규정하고 있다. 또 규칙에서는 ① 환자의 의료정보에 대한 3가지 권리(권리개시청구권·정정청구권·설명보고권), ② 환자 프라이버시 침해 시 민·형사 처벌, ③ 공중위생·의학연구 등 국가적 우선사항에 대한 프라이버시권의 공적 의무, ④ 의료정보중 환자의 신원정보 사용의 의료목적 내 제한, ⑤ 의료정보 수탁기관의 프라이버시 보호시스템 및 절차 수립 등을 원칙으로 정하고 있다.[22]

⑵ 독일: 당사자의 명문상 동의 또는 응급상황을 제외하고 정보공개 등을 원칙적으로 금지하는 EU 정보보호지침(European Community Directive on Data Protection)을 수용한 연방정보보호법(Bundesdatenschutzgesetz, 2001)에서 대체로 의료정보를 일반 정보의 한 유형으로 보는 관점에서 다루고 있다. 이 법에서는 특별한 개인정보로서 건강에 관한 정보(제3조 제9항), 환자의 건강을 위한 의사의 의료정보 수집 및 비밀보호(제28조 제7항) 등에 관해 규정하고 있다. 그밖에 표준직업법(Musterberufsordnung) 제15조 제1항의 '의사의 기록' 의무와 보존연한에 관한 규정, 연방의사법(Deutsch

---

22) 백윤철, "미국의 개인정보보호와 HIPAA", 『미국헌법연구』, 제19권 제1호, 미국헌법학회, 2008. 2, 제85~94면; 김진경·한우석, "의료정보 이용 및 공개에 관한 법적 기준-미국 프라이버시규칙과 피험자보호규칙의 검토", 『한양법학』, 제20권 제4호, 한양법학회, 2009. 11, 제211~220면 참조.

Medizinrecht) 제2조 제5항의 의사의 치료행위에 관한 규정, 연방암등록법(Bundeskrebsregistergesetz, 1995)의 의료정보 관련규정, 사회법전 제10편의 의료보험상 사회정보의 특별한 범주로서 의료정보 관련규정 등이 있다.[23]

2. 우리나라의 보건의료정보 법제

⑴ 헌법: 우리나라의 보건의료정보 법제는 헌법을 최상위법으로 하고 이를 근간으로 아래에서 기술하는 민·형사법, 보건의료관련법, 정보통신 관련법 등 여러 개별 실정법에서 관련 조항들을 규정하여 규율하는 방식을 갖추고 있다. 보건의료정보는 개인정보의 한 유형이라는 점에서 헌법상 기본권으로서 개인정보자기결정권 또는 자기정보통제권(the Right to Informational Self-Determination)에 근거하는 것이며, 구체적으로 이 개인정보자기결정권의 법적 근거는 헌법 제17조(사생활의 비밀과 자유), 제10조(인격권·행복추구권), 제18조(통신의 비밀), 제21조 제1항(언론·출판의 자유, 알권리)에서 찾을 수 있다.[24]

⑵ 민·형사법: 의료행위에 관한 계약불이행 또는 불법행위로 인한 손해배상책임을 규정한 민법 제390조(채무불이행과 손해배상), 제750조(불법행위의 내용)와 의료행위로 인한 형사처벌을 규정한 형법 제317조(업무상비밀누설), 제316조(비밀침해), 제127조(공무상 비밀 누설), 제347조의2(컴퓨터 사용사기) 등이 환자의 비밀 또는 개인정보를 보호하고 처벌하는 민·형사상 책임규정이다.

⑶ 보건의료 관련법: 보건의료기본법 제13조(비밀보장) 및 제12조(보건의료서비스에 관한 자기결정권), 제11조(보건의료에 관한 알권리)가 여러 보건

---

23) 김상겸, "독일의 의료정보와 개인정보 보호에 관한 연구", 『한독사회과학논총』, 제15권 제2호, 한독사회과학회, 제3~13면 참조.

24) 헌법재판소 2005.5.26. 선고 99헌마513 결정; 헌법재판소 2007.5.31. 선고 2005헌마1130 결정 참조.

의료관련법에서 보건의료정보 보호의 근간이 되는 법률이다. 그리고 의료법 제23조 제3항(전자의무기록), 제18조 제3항(처방전 작성과 교부), 의료법 제19조(비밀누설금지), 의료법 제21조(기록열람 등) 등에서 규정하는 진료기록부(의무기록)·전자의무기록 및 전자처방전 관련 조항이 대표적인 법률이다. 그밖에 개별법으로는 장기 등 이식에 관한 법률, 정신보건법, 후천성면역결핍증 예방법, 의료기사 등에 관한 법률, 국민건강보험법, 감염병의 예방 및 관리에 관한 법률, 결핵예방법, 혈액관리법, 암관리법, 모자보건법, 생명윤리 및 안전에 관한 법률, 노인 장기요양보험법, 의료사고 피해구제 및 의료분쟁조정 등에 관한 법률, 산업안전보건법, 약사법 등에도 보건의료정보를 보호하는 관련 규정을 두고 있다.

⑷ 정보통신 관련법: 개인정보를 보호하는 대표적인 법제로는 개인정보보호법(2011.3.29. 제정, 2011.9.30. 시행)이 있다. 종전에는 정보통신 관련 법제 가운데 국·공립 의료기관에는 공공기관의 개인정보보호에 관한 법률이 적용되고 민간 의료기관에는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(동법 시행규칙 제6조 제11호에 근거)이 각각 적용됐으나 공공기관의 개인정보보호에 관한 법률이 개인정보보호법으로 전면 대체 입법되어 모든 의료기관에 적용될 수 있게 됐다.[25] 그밖에 전자서명법, 신용정보의 이용 및 보호에 관한 법률 등에서도 개인정보 보호 관련 규정을 두고 있다. 한편, 보건복지부에서는 개인정보보호법 제12조 제2항에서 그 법적 근거를 찾을 수 있는 '의료기관 개인정보보호 가이드라인(500병상 이상 의료기관 대상)'을 제정·공포하여 2010.3.15일부터 시행하고 있다.

특히, 개인정보보호법은 양벌규정으로 위반 시 개인과 법인 모두가 처벌을 받게 되기 때문에 특히 의료기관의 실무적인 측면에서는 형사처벌을 규정한 다음 3개 조항 및 12개 벌칙사항을 숙지하고 실천할 필요가 있다.

① 정보주체의 동의 없이 개인정보를 제3자에게 제공 또는 그 사정을 알고

25) 정보통신망 이용촉진 및 정보보호 등에 관한 법률은 일부 규정을 삭제하고 법 자체는 존속하고 있다.

도 개인정보를 제공받은 경우, ② 영리 또는 부정한 목적으로 개인정보를 제공받은 경우, ③ 사생활을 침해할 우려가 있는 민감정보를 처리한 경우, ④ 정보주체의 동의 없이 고유 식별정보를 처리한 경우, ⑤ 업무상 알게 된 개인정보를 누설하거나 타인에게 제공한 경우, ⑥ 정당한 권한 없이 타인의 개인정보를 훼손·멸실·유출한 경우(이상 위반 시 5년 이하 징역 또는 5천만 원 이하 벌금: 제71조), ⑦ 영상정보처리기기를 설치목적 외 임의로 조작하거나 녹음한 경우, ⑧ 부정한 수단으로 개인정보를 취득하거나 제공받은 경우, ⑨ 직무상 알게 된 비밀을 누설하거나 직무상 목적 외로 이용한 경우(이상 위반 시 3년 이하 징역 또는 3천만 원 이하 벌금: 제72조), ⑩ 안전성 확보에 필요한 조치 없이 개인정보를 분실·도난·유출한 경우, ⑪ 정정·삭제에 필요한 조치 없이 개인정보를 계속 이용한 경우, ⑫ 개인정보처리를 정지하지 않고 계속 이용하거나 제3자에게 제공한 경우(이상 위반 시 2년 이하 징역: 제73조).

⑸ 건강정보보호법 입법 추진현황 : 개인정보에 관해 의료기관을 포함한 모든 보건의료분야에 특정해서 적용하기 위한 일반법으로 개인건강정보보호법(가칭)의 입법 작업이 2006.10월부터 추진되었으나 2011.12월 현재 국회에 계류 중에 있다.[26] 그런데 이 법의 입법과정에서 가장 큰 쟁점이 된 것은 개인건강정보 즉 보건의료정보의 공유 또는 공동 활용으로 인해 얻을 수 있는 사회적 편익과 그에 따른 개인의 프라이버시 침해 발생 가능성이 동시에 존재한다는 점이 문제점으로 제기된바 있다. 이러한 점에서 이 법안의 적용범위는 의료기관에서 생성되는 환자의 진료정보에 초점을 맞추는 것보다 의료기관 이외에서 생성되는 각종의 보건의료정보 즉, 보건의료기본법에서 정의하고 있는 넓은 의미에서의 보건의료정보까지를 포괄하는 것이 타당하며, 특히 미래의 의료환경인 원격진료 또는 u-헬스 시대를 감안한다면 이러

26) (가칭) 개인건강정보보호법 입법안에 대한 상세내용에 관해서는 이진영, "보건의료분야에서의 자기정보통제권", 『생명윤리정책연구』, 제3권 제2호, 생명윤리정책연구센터, 2009, 제179~196면 참조.

한 보건의료정보 내지 디지털보건의료정보가 정보통신망을 통해 언제 어디서나 공유될 수 있다는 점을 염두에 두고 이를 대비한 포괄적인 법제화가 이루어지는 것이 바람직하다고 본다.

IV. 보건의료정보의 보호

1. 정보보호의 법적 근거

의료기관 내부 또는 외부에서 보건의료정보의 침해는 그 생성, 저장 및 보존, 이용, 폐기 등 각각의 처리단계에서 분실·유출·도난·위조·변조·훼손·악용·오용·남용 등 다양한 형태로 나타날 수 있기 때문에 이를 보호하는 장치가 필요하다. 여기서 개인정보보호법 제2조[27]에 따르면, 개인정보의 '처리'란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 의미한다. 또 개인정보처리자란 업무를 목적으로 개인정보파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관, 법인, 단체 및 개인을 말한다.

의료법상 환자의 비밀유지 및 의료정보(개인정보) 보호의무는 의사의 직업윤리(묵비의무)와 의료계약상 의무이며, 그 근원은 헌법상 도출되는 개인정보자기결정권에 근거한다. 개인정보자기결정권이란 정보의 조사·취급·처리의 형태나 정보의 내용을 불문하고 그 자신에 관해 무엇인가를 말해주는 정보를 누군가가 조사·처리해도 되는지 여부와 그 시기·방법·범위·목적 등에 대하여 그 정보의 주체가 자율적으로 결정하고 관리할 수 있는 권리를 말한다. 이는 소극적 방어권이자 적극적 청구권으로서의 성격을 가지며, 원칙적으로 생존하고 있는 자연인만이 주체가 될 수 있으나 사회통념상 수인한도

---

27) 개인정보보호법 제2조 제2호, 제5호.

를 벗어날 정도로 명예와 신용이 훼손된 경우에는 예외적으로 법인도 그 주체가 될 수 있다.

이 권리에 근거하여 정보주체는 자신의 개인정보에 대한 ① 수집단계에서 수집통제권(수집동의권), ② 저장 및 보존단계에서 보유통제권(개인정보열람청구권·개인정보정정청구권·개인정보삭제청구권), ③ 활용단계에서 이용 및 제공통제권(침해중단청구권·추가적동의권·개시동의권)을 가진다. 이와 관련하여 개인정보보호법에서는 5가지 항목의 정보주체의 권리를 규정하고(제3조), 구체적으로 개인정보의 열람(제35조), 정정·삭제(제36조), 처리정지(제37조), 손해배상청구(제39조) 등에 관한 상세한 규정을 두고 있다.

2. 기술적, 물리적 보호

보건의료정보처리자(개인정보취급자·개인정보취급의료기관: 이하 '개인정보처리자'와 동일한 의미로 사용함)는 개인정보보호법과 의료법 및 의료기관 개인정보보호 가이드라인(보건복지부)에 따라 기술적, 물리적 측면에서 보건의료정보의 안전성 및 신뢰성을 담보할 수 있는 시설 및 장비를 구비해야 한다.

의료법에 따르면, 의료인 또는 의료기관개설자는 보건복지부령이 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는데 필요한 시설 및 장비를 갖추어야 한다.[28] 그 구체적인 기준으로는 전자의무기록의 생성과 전자서명을 검증할 수 있는 장비, 전자서명이 있은 후 전자의무기록의 변경여부를 확인할 수 있는 장비, 네트워크에 연결되지 아니한 백업저장시스템으로 규정하고 있다.[29] 다시 말하자면, 전자의무기록이 작성·보존·재생되는 컴퓨터 및 그와 연결된 다른 컴퓨터 또는 네트워크에 대하여 최소한의 합리적 보안조치를 해야 하고 의료기관내 또는 밖으로 전자의무기록을 전송할 경우

28) 의료법 제23조 제2항.
29) 의료법시행규칙 제16조.

그 전송과정에서 내용이 유출되지 않도록 암호시스템을 갖추어야 한다(기밀성: confidentiality). 또한 위조와 변조를 방지하고(무결성: integrity: verification) 작성자의 신분을 증명하며(진정성: authenticity) 사후에 부인하지 못하도록(부인봉쇄: non-repudiation) 전자서명법 제3조에 의한 공인전자서명을 하도록 의무화하고 있다. 여기서 전자서명이란 서명자를 확인하고 서명자가 당해 전자문서에 서명했음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다. 그런데 현행 법제상 이러한 시설 및 장비를 구비하지 않은 경우 그 벌칙규정이 없을 뿐 아니라 시설 및 장비의 구체적인 품질규격(HL7, DICOM, IHE 등)[30]을 상세하게 규정하고 있지 않는 것은 디지털보건의료정보의 민감성 및 중요성에 비추어 볼 때 입법적으로 개선되어야 할 점이다.

한편, 실무적으로 보건의료정보처리자는 의료기관 개인정보보호 가이드라인(보건복지부)에 근거하여 다음과 같은 조치를 시행해야 한다.[31] ① 전자매체장치 설치장소에 대해 물리적 시설기준을 충족하는 개인정보보호구역 설정, ② 정보시스템의 운영 및 보안관리 절차 마련, ③ 정보시스템의 도입 및 변경에 관한 절차 문서화, ④ 유·무선 네트워크에 대한 접근통제·보안관리 절차 수립, ⑤ 의료정보시스템 사용에 대한 로그모니터링 절차 수립 및 주기적 검토, ⑥ 악성코드 모니터링 또는 접근제한 방법을 활용한 정보유출 방지, ⑦ 백업 및 문서화된 복구절차 마련, ⑧ 직종별·업무별·개인별 보안수준 및 접근권한 문서화, 사용자 및 작업로그 관리, ⑨ 의료정보시스템 사용자지침 수립, ⑩ 의료정보 보안사고 예방 및 대응계획 수립, ⑪ 의료정보시스템 프로그램 개발지침 수립 및 명세화, ⑫ 의료법 제21조 제3항에 따른 진료정

30) 송지은·김신효·정명애, "u-헬스케어 서비스에서의 의료정보보호", 『정보보호학회지』, 제17권 제1호, 한국정보보호학회, 2007.2, 제50~54면; 김성현·김민우·오암석·김관형·강성인, "u-헬스케어 시스템의 의료정보 표준화 기술에 관한 연구", 『한국멀티미디어학회 추계학술발표대회 논문집』, 제13권 제2호, 한국멀티미디어학회, 2010, 제208~209면 참조.

31) 보건복지부, 『의료기관 개인정보보호 가이드라인(500병상 이상 의료기관 대상)』, 2010. 3, 제13~29면.

보 교환지침 수립, ⑬ 조직 전반에 걸친 암호화통제정책 수립, ⑭ 의료정보 침해사고 유형별 대응요령 숙지 등 보안관제 활동 시행.

그런데, 개인정보보호법 및 보건복지부 가이드라인의 시행 초기인 현재 상황에서는 개별 의료기관들이 환자의 개인정보에 대한 기술적·물리적 보호조치를 위한 노력이 이루어지고 있으나 미흡한 점이 많은 것으로 파악되고 있다. 예컨대 내부구성원(의료진·기타 종사자)의 개별 환자정보에 대한 접근권한 통제는 비교적 잘 이루어지고 있는 반면, 의료정보시스템에 대한 컴퓨터보안감사 및 외부안전진단 실시, 의료정보보안사고 예방 및 대응교육의 정기적 실시, 다른 의료기관 등 외부 기관과의 진료정보교환 또는 전송에 따른 보안방안 및 책임을 정한 지침 수립 및 실행 등은 원활하지 않은 실정이다. 앞으로 보건복지부 등 감독기관의 정기적인 감사 및 점검시스템이 마련되고 실질적인 시행이 필요하다고 본다.

3. 관리적 보호

보건의료정보처리자는 개인정보보호법에 따라 안전조치의무(제29조), 개인정보처리방침 수립 및 공개(제30조), 개인정보보호책임자 지정(제31조) 등 개인정보의 안전한 관리를 위한 조치를 하여야 한다. 또한 개인정보가 유출되었음을 알게 되었을 때에는 유출된 개인정보의 항목, 유출시점과 그 경위, 발생 가능한 피해를 최소화하기 위해 정보주체가 할 수 있는 방법, 개인정보처리자의 대응조치 및 피해구제 절차, 신고접수 담당부서 및 연락처를 지체 없이 해당 정보주체에게 통지해야 한다(제34조). 그밖에 공공기관에 해당하는 국·공립 의료기관의 장은 개인정보파일의 등록 및 공개(제32조), 개인정보영향평가(제33조)를 실시해야 한다.

또한, 구체적으로는 의료기관 개인정보보호 가이드라인(보건복지부)에 따라 관리적 측면에서 보건의료정보에 대하여 다음과 같은 보호조치를 시행해야 한다.[32] 첫째, 의료기관은 개인정보보호위원회를 운영하고 위원회운영

규정과 개인정보보호규정을 수립하고, 개인정보관리책임자 1인, 개인정보보호(privacy) 실무책임자 및 개인정보보안(security) 실무책임자 각 1인(전임자 1인 필수)을 지정해야 한다. 둘째, 인적 자원의 채용 및 직무 수행에 있어 정보보호규정과 보안서약서를 준수하도록 교육 및 훈련을 정기적으로 실시해야 한다. 셋째, 정보자산을 전자정보자산·문서정보자산·시스템자산·시설자산 등으로 분류하여 목록화 하고, 업무 중 수집·이용·제공되는 모든 개인정보의 취급내역을 파악하여 개인정보일람표로 목록화 하고 이를 관리해야 한다.

그런데, 개인정보보호법과 보건복지부 가이드라인의 시행 초기인 현재 시점에서는 환자의 개인정보에 대한 관리적 보호조치가 미흡한 점이 발견된다. 실제로 개별 의료기관에서 개인정보보호위원회를 설치하여 정기적으로 운영하는 체계를 갖추고 있지 못하고, 특히 개인정보관리책임자·개인정보보호실무책임자·개인정보보안실무책임자 각 1인을 임명 또는 채용하여 정보보호업무를 전담해서 수행하도록 하는 의료기관이 많지 않은 실정이다. 후자의 이유로는 기존의 전산팀 또는 의료정보센터 인력 이외에 추가로 정보보호 전문인력을 충원하는데 따르는 인건비가 부담으로 작용하는 것으로 생각된다. 전술한 기술적·물리적 보호조치의 경우와 마찬가지로 보건복지부 등 감독기관의 정기적인 감사 및 점검시스템이 시급히 갖추어져야 할 것이다.

4. 법제도적 보호

보건의료정보에 대한 법제도적 측면의 보호조치는 전술한 바와 같이 의료법과 기타 특별법 및 개인정보보호법 등에서 환자의 비밀 또는 개인정보 보호의무 및 위반 시 벌칙규정을 정하고 있는 것이 그것이다(아래 <표 4-1>).

의료법 제19조는 의료인이 의료·조산·간호를 하면서 알게 된 다른 사람의 비밀을 누설하거나 발표하지 못하도록 금지하고, 제22조 제3항에서 진료

32) 보건복지부, 전게서, 제3~12면.

기록부 등을 거짓으로 작성하거나 고의로 사실과 다르게 추가 기재·수정하지 못하도록 금지하고 있다(2012.4.8. 시행). 또 의료법 제23조 제3항 및 제18조 제3항은 누구든지 정당한 사유 없이 전자의무기록 또는 전자처방전에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다고 규정하고 있다. 그런데 의료법상 비밀보호는 의료인을 대상으로 하여 '환자의 비밀 또는 진료기록부 작성내용'만을 보호하며 이를 위반하는 경우 3년 이하 징역 또는 1천만 원 이하 벌금에 처한다고 규정하고 있다(의료법 제19조, 제22조 제3항, 제88조). 이에 비해, 개인정보보호는 '누구든지'라고 표현하여 행위주체를 모든 의료종사자 및 일반인에게 확대하고 그 보호객체도 비밀보다 확장된 '환자의 개인정보(보건의료정보)'까지 보호하며 이를 위반하는 경우 '5년 이하 징역 또는 2천만 원 이하 벌금'(의료법 제23조 제3항, 제18조 제3항, 제87조)에 처한다고 규정하고 있다.

그런데, 개인정보보호법 제23조에서는 민감정보의 종류를 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보라고 적시하면서 보건의료정보에 해당하는 '건강정보'를 함께 열거하고 있고 이들 개인정보에 대한 처리를 특별히 제한하는 한편, 동법 제71조에서는 이를 위반하는 경우 '5년 이하 징역 또는 5천만 원 이하 벌금'에 처하도록 규정하고 있다. 여기서 말하는 민감정보에 해당하는 '건강정보'와 의료법 제23조 제3항 및 제18조 제3항에서 말하는 '환자의 개인정보'는 동일한 범주에 해당하는 것으로 볼 수 있는바, 민감정보로 동일시되는 건강정보와 환자의 개인정보에 대해 두 실정법에서 처벌조항에 차이를 두고 있는 모순이 발견된다. 한편, 형법 제316조 제2항에서는 봉함 기타 비밀장치한 사람의 편지·문서·도화 또는 전자기록 등 특수매체기록에 대한 비밀을 침해한 경우 '3년 이하 징역이나 금고 또는 500만 원 이하 벌금'에 처하도록 규정하고 있다. 여기서 말하는 '전자기록 등 특수매체기록'은 의료법 제23조의 전자의무기록에 해당하는 것으로 의료법이 형법보다 가중처벌 하고 있는 것은 의무기록 비밀의 보호법익이 다른

기록의 보호법익보다 큰 것으로 판단하고 있다는 견해[33]도 타당하다고 본다. 생각건대, 의료법상 환자의 개인정보 보호의무 위반에 대한 벌칙규정을 개인정보보호법상 민감정보인 건강정보의 벌칙 수준으로 상향해서 양자를 일치시키도록 하는 의료법 개정이 필요하다고 본다.

또한, 아래 <표 4-1>에서 법규들을 비교해서 살펴보면 개인정보의 침해양태와 그 벌칙정도가 예컨대 같은 '비밀누설'인 경우에도 각각의 실정법마다 차이가 있고 일정한 규칙성도 보이지 않는다는 것을 알 수 있다. 그런데 모두가 의료행위 과정에서 생성되는 보건의료정보에 대한 침해라고 한다면 적어도 보건의료 관련 법제들 사이에서는 벌칙 정도가 어느 정도 규칙성 내지 형평성을 가져야 할 것으로 생각하는바, 이에 대한 상세한 사항은 추후 연구에서 검토하고자 한다.

<표 4-1> 주요 법률상 보건의료정보의 보호 및 벌칙규정

법률명	보호규정	벌칙규정
민법	제390조(채무불이행과 손해배상) 제750조(불법행위의 내용)	손해배상책임 손해배상책임
형법	제317조(업무상비밀누설) 제316조(비밀침해) 제127조(공무상비밀누설) 제347조의2(컴퓨터 사용사기)	3년 이하 징역이나 금고, 10년 이하 자격정지 또는 700만 원 이하 벌금 3년 이하 징역이나 금고 또는 500만 원 이하 벌금 2년 이하 징역이나 금고 또는 5년 이하 자격정지 10년 이하 징역 또는 2천만 원 이하 벌금
의료법	제23조 제3항(전자의무기록) 제18조 제3항(처방전작성과 교부) 제19조(비밀누설금지) 제69조 제3항(의료지도원) 제21조(기록열람 등) 제22조 제3항(진료기록부등 수정) [시행예정]	(제87조) 5년 이하 징역 또는 2천만 원 이하 벌금 (제87조) 5년 이하 징역 또는 2천만 원 이하 벌금 (제88조) 3년 이하 징역 또는 1천만 원 이하 벌금 (제88조) 3년 이하 징역 또는 1천만 원 이하 벌금 (제88조) 3년 이하 징역 또는 1천만 원 이하 벌금, (제90조) 300만 원 이하 벌금 (제88조) 3년 이하 징역 또는 1천만 원 이하 벌금
장기 등 이식에 관한 법률	제31조(비밀의 유지)	(제49조) 3년 이하 징역 또는 2천만 원 이하 벌금
정신 보건법	제42조(비밀누설의 금지)	(제56조) 3년 이하 징역 또는 1천만 원 이하 벌금

33) 조형원, "유비쿼터스 보건의료서비스 활성화지원 법률안의 제안", 『의료법학』, 제10권 제1호, 대한의료법학회, 2009, 제184~185면.

응급 의료에 관한 법률	제40조(비밀준수의무)	(제60조) 5년 이하징역 또는 3천만 원 이하 벌금 (제55조) 면허·자격취소 또는 6개월 정지
후천성 면역결핍증 예방법	제7조(비밀누설금지)	(제26조) 3년 이하 징역 또는 1천만 원 이하 벌금
의료기사 등에 관한 법률	제10조(비밀누설의 금지)	(제30조) 3년 이하 징역 또는 1천만 원 이하 벌금
국민건강보험법	제86조(비밀의 유지)	(제94조) 3년 이하 징역 또는 3천만 원 이하 벌금
감염병의 예방 및 관리에 관한 법률	제74조(비밀누설의 금지)	(제78조) 3년 이하 징역 또는 3천만 원 이하 벌금
결핵 예방법	제29조(비밀누설금지)	(제31조) 3년 이하 징역 또는 3천만 원 이하 벌금
혈액 관리법	제7조의2 제5항(채혈금지대상자의 관리) 제12조 제3항(기록의 작성) 제12조의2 제3항(전자혈액관리업무 기록등)	(제19조) 2년 이하 징역 또는 500만 원 이하 벌금 (제19조) 2년 이하 징역 또는 500만 원 이하 벌금 (제19조) 2년 이하 징역 또는 500만 원 이하 벌금
암 관리법	제49조(개인정보의 목적 외 사용금지) 제44조(비밀유지의무)	(제51조) 3년 이하 징역 또는 1천만 원 이하 벌금 (제51조) 3년 이하 징역 또는 1천만 원 이하 벌금
모자 보건법	제24조(비밀누설의 금지)	(제26조) 1년 이하 징역 또는 1천만 원 이하 벌금
노인 장기요양보험법	제62조(비밀누설금지)	(제67조) 2년 이하 징역 또는 1천만 원 이하 벌금
산업안전보건법	제63조(비밀유지) 제52조의6(비밀유지)	(제68조) 1년 이하 징역 또는 1천만 원 이하 벌금 (제68조) 1년 이하 징역 또는 1천만 원 이하 벌금
약사법	제87조(비밀누설금지)	(제94조) 3년 이하 징역 또는 1천만 원 이하 벌금
생명윤리 및 안전에 관한 법률	제35조(유전정보 등의 보호) 제35조의2(유전정보 등의 관리) 제48조(비밀누설 등의 금지)	(제52조) 2년 이하 징역 또는 3천만 원 이하 벌금 (제53조) 1년 이하 징역 또는 2천만 원 이하 벌금 (제51조) 3년 이하 징역
의료사고 피해구제 및 의료분쟁 조정 등에 관한 법률	제41조(비밀누설의 금지)	(제53조) 3년 이하 징역 또는 1천만 원 이하 벌금
개인정보보호법	제59조 3호(금지행위) 외 제39조(손해배상책임)	(제71조) 5년 이하 징역 또는 5천만 원 이하 벌금 손해배상책임
전자 서명법	제24조(개인정보의 보호) 제26조(배상책임)	손해배상책임

한편, 개인정보보호법은 제3조에서 개인정보처리자의 개인정보보호 8원

칙을 규정하면서 그 생명주기 단계별로 다음과 같은 법적 보호규정을 두고 있다.

⑴ 개인정보의 수집·이용: 개인정보처리자는 다음 6가지 경우 개인정보를 수집하고 그 수집목적의 범위에서 이용할 수 있다. ① 정보주체의 동의를 받은 경우, ② 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위해 불가피한 경우, ③ 공공기관이 법령 등에서 정하는 소관업무의 수행을 위해 불가피한 경우, ④ 정보주체와의 계약 체결 및 이행을 위해 불가피하게 필요한 경우, ⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명·신체·재산의 이익을 위해 필요하다고 인정되는 경우, ⑥ 개인정보처리자의 정당한 이익을 달성하기 위해 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우(제15조).

⑵ 개인정보의 제공: 개인정보처리자는 정보주체의 동의를 받은 경우에는 상기 ②, ③, ⑤항에 따라 수집목적 범위에서 개인정보를 제공하는 경우에는 개인정보를 제3자에게 제공할 수 있다(제17조).

⑶ 개인정보의 수집·이용·제공 제한: 개인정보를 수집하는 경우에도 그 목적에 필요한 최소한의 개인정보를 수집해야 한다(제16조). 또한 개인정보처리자는 범위를 초과하여 이용하거나 제3자에게 제공해서는 아니 된다(제18조 제1항). 다만, 정보주체로부터 별도의 동의를 받은 경우와 다른 법률에 특별한 규정이 있는 경우 등 9가지 경우에는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 있다(제18조 제2항).

⑷ 개인정보의 파기: 개인정보처리자는 다른 법령에 따라 보존해야 하는 경우를 제외하고는 보유기간의 경과, 개인정보 처리목적의 달성 등 그 개인정보가 불필요하게 되었을 때에는 복구 또는 재생되지 않도록 조치한 후 지체 없이 이를 파기해야 한다(제21조). 개인정보의 파기방법은 동법 시행령 제16조에 따라야 한다.

⑸ 동의를 받는 방법: 개인정보처리자는 정보주체의 동의를 받을 때에는

각각의 동의사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다(제22조 제1항). 그리고 개인정보 수집·이용 및 제공 동의, 민감정보 및 고유 식별정보 처리 동의의 경우에는 정보주체의 동의 없이 처리할 수 있는 개인정보와 동의가 필요한 개인정보를 구분하여야 한다(제22조 제2항).

⑹ 개인정보의 처리 제한: 개인정보처리자는 민감정보(제23조) 및 고유 식별정보(제24조)의 경우에는 다른 개인정보 처리의 동의와 별도로 동의를 받은 경우 또는 법령에서 처리를 요구하거나 허용하는 경우를 제외하고는 처리해서는 아니 된다.(제26조). 한편, 영업양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 이전하려는 사실, 이전받는 자의 성명·주소·전화번호·연락처, 정보주체가 이전을 원하지 않는 경우 조치방법 및 절차를 서면 등의 방법으로 미리 정보주체에게 알려야 한다(제27조).

다만, 환자의 개인정보인 보건의료정보의 이관에 대해서는 일반 개인정보와는 달리 의료법 제40조 제2항 및 동법 시행규칙 제30조 제4항에서 특별규정을 두고 있다. 즉, 의료기관개설자가 폐업 또는 휴업신고를 할 때에는 기록·보존하고 있는 진료기록부 등을 관할 보건소장에게 이관해야 하며, 다만 의료기관개설자가 직접 보관하고자 하는 경우에는 그 보관계획서를 관할 보건소장에게 제출하여 허가를 받아야 한다. 그런데 폐업 또는 휴업한 의료기관의 환자가 다른 의료기관에서 계속 진료를 받기 위해 진료기록부 사본을 교부받아야 하는 경우 보건소나 직접 보관하는 의료기관개설자의 보존상태 여하에 따라 용이하지 않은 사례가 많다는 조사결과가 나왔다.[34] 이와 같은 결과는 현행법상 전술한 바와 같이 보건소 이관과 의사 직접 보관 조항을 두

34) 최근 국민권익위원회가 전국 20개 보건소에 대해 실태조사를 한 결과, 보건소는 장소 및 인력 부족을 이유로 진료기록 보관을 사실상 의료기관개설자에게 넘기는 경우가 많았다(보건소 보관 비율 1.6%, 의료기관개설자 보관 비율 98.4%). 또 진료기록을 직접 보관하는 폐·휴업 의료기관개설자는 연락처가 바뀌어도 보건소에 제대로 신고하지 않는 경우가 빈번했고 폐업병원의 원무과장·사무장이 보관하는 등 진료기록 관리가 사실상 방치된 경우도 있었다(뉴시스, “휴·폐업중인 병원 진료기록부 발급 쉬워진다”, 12.6. 2012 <www.newsis.com>).

면서도 위반 시 제재조치로는 보건복지부장관 또는 시장·군수·구청장이 의료업 정지, 개설허가 취소, 의료기관 폐쇄를 명하거나(의료법 제64조 제1항 5호) 이관하지 아니한 의사에게 100만 원 이하 과태료를 부과(의료법 제92조 제3항 3호)하는 정도에 그치고 있기 때문이다. 생각건대, 우선 행정적으로 보건소 보존관리시스템을 충분히 재정비하고 보건소가 폐업·휴업한 의사의 소재지 및 직접 보관중인 진료기록부의 보존상태를 체계적으로 파악할 수 있는 점검 및 보고시스템을 갖출 필요가 있다. 또한 의료법 제22조 제2항에서 정하는 진료기록부 보존의무를 위반한 경우 300만 원 이하 벌금에 처하도록 하는 규정(의료법 제90조)과 같이 폐·휴업 시 진료기록부 이관 및 직접 보존 의무도 여기에 준하는 것으로 간주하고 의료법 제90조 수준의 벌칙조항을 신설하는 것도 효과적인 방법이라고 생각한다.

V. 보건의료정보의 열람 및 교부

1. 정보열람 등의 법적 근거

환자의 개인정보 내지 보건의료정보의 법적 근거가 되는 개인정보자기결정권은 헌법 제37조 제2항의 기본권의 제한원리에 따라 열람 또는 교부될 수 있다. 즉, 개인정보자기결정권은 국가안전보장, 질서유지, 공공복리를 위해 필요한 경우 법률에 의하여 세 가지 원칙(비례원칙·규범명확성원칙·목적구속성원칙) 하에 제한될 수 있다. 이에 따라 전술한 개인정보보법 제15조, 제17조, 제18조 제2항에서 정하는 바와 같이 개인정보의 이용, 제공, 목적 외 이용 및 제공 등이 가능하다. 그리고 개인정보보호법 제35조에서 정보주체의 개인정보 열람요구권을 보장하는 한편, 개인정보처리자가 열람을 제한 및 거절할 수 있는 경우를 적시하고 있다. 또한 보건의료기본법 제11조에 따라 모든 국민은 보건의료인 또는 보건의료기관에 대해 자신의 보건의료와 관련한 기록 등의 열람이나 사본교부를 요청할 수 있으며, 의료법 제21조 등에

서도 의무기록의 열람 및 사본교부 요구권 등을 법제화하고 있다.

2. 보건의료정보의 열람 및 교부제도

가. 정보주체 및 그 가족 등에 의한 열람 및 교부

의료법 규정에 따라 환자는 의료인 또는 의료기관 종사자에 대해 자신의 기록을 열람하거나 사본의 교부를 요구할 수 있다(제21조 제1항). ① 다만 환자의 배우자, 직계 존·비속, 배우자의 직계존속(또는 환자가 지정하는 대리인)이 환자본인의 동의서와 친족관계임을 나타내는 증명서(또는 대리권 있음을 증명하는 서류) 등을 첨부하는 등 보건복지부령으로 정하는 요건(요청자의 신분증, 가족관계증명서 또는 주민등록표등본 등, 위임장, 환자의 자필서명 동의서 및 신분증)을 갖추어 요청한 경우, ② 환자가 사망하거나 의식이 없는 등 동의를 받을 수 없어 그 배우자, 직계 존·비속, 배우자의 직계존속이 친족관계임을 나타내는 증명서 등을 첨부하는 등 보건복지부령으로 정하는 요건을 갖추어 요청한 경우에는 그 요청자에게 기록열람 또는 사본교부를 할 수 있다(제21조 제2항 1호~3호). 한편, 의사·치과의사·한의사 또는 조산사는 자신이 진찰·검안 또는 조산한 환자가 진단서·검안서·증명서 또는 출생·사망·사산증명서의 교부를 요청하는 경우 정당한 사유 없이 이를 거부하지 못한다(제17조 제3항~제4항).

나. 법률의 규정에 의한 열람 및 교부

이하에서 열거하는 각 법률의 규정에 근거하여 환자 개인의 보건의료정보는 열람 및 교부될 수 있다.

① 국민건강보험법 제13조, 제43조, 제43조의2, 제56조에 따라 급여비용의 심사·지급·대상여부 확인·사후관리 및 요양급여의 적정성평가·가감지급 등을 위해 국민건강보험공단 또는 건강보험심사평가원에 제공하는 경우, ② 의료급여법 제5조, 제11조, 제11조의3, 제33조에 따라 의료급여 수급권자

확인, 급여비용의 심사·지급, 사후관리 등 의료급여업무를 위해 보장기관(시·군·구), 국민건강보험공단, 건강보험심사평가원에 제공하는 경우, ③ 형사소송법 제106조, 제215조, 제218조에 따른 경우(법원의 압수, 검사 또는 사법경찰관의 압수·수색·검증·영장에 의하지 아니한 압수), ④ 민사소송법 제347조에 따라 문서제출을 명한 경우(문서송부명령), ⑤ 산업재해보상보험법 제118조에 따라 근로복지공단이 보험급여를 받는 근로자를 진료한 산재보험 의료기관에 대해 그 근로자의 진료에 관한 보고 또는 서류 등의 제출을 요구하거나 조사하는 경우, ⑥ 자동차손해배상보장법 제12조 제2항, 제14조에 따라 의료기관으로부터 자동차보험진료수가를 청구 받은 보험회사 등이 그 의료기관에 대해 관계 진료기록의 열람을 청구한 경우, ⑦ 병역법 제11조의2에 따라 지방병무청장이 징병검사와 관련하여 질병 또는 심신장애의 확인을 위해 필요하다고 인정하여 의료기관의 장에게 징병검사대상자의 진료기록·치료관련 기록의 제출을 요구한 경우, ⑧ 학교안전사고 예방 및 보상에 관한 법률 제42조에 따라 공제회가 공제급여의 지급 여부를 결정하기 위해 필요하다고 인정하여 국민건강보험법 제40조에 따른 요양기관에 대해 관계 진료기록의 열람 또는 필요한 자료의 제출을 요청하는 경우, ⑨ 고엽제후유의증 환자지원 등에 관한 법률 제7조 제3항에 따라 의료기관의 장이 진료기록 및 임상소견서를 보훈병원장에게 보내는 경우, ⑩ 의료사고 피해구제 및 의료분쟁 조정 등에 관한 법률 제28조 제3항에 따라 의료사고 조사를 위한 경우(2012.4.8. 시행)(의료법 제21조 제2항 4호~13호).

다. 환자이송 등에 따른 의료정보 교환

의료법에 따르면, 의료인은 다른 의료인으로부터 진료기록의 내용 확인이나 진료경과에 대한 소견 등을 송부할 것을 요청 받은 경우에는 해당 환자나 그 보호자의 동의(환자가 의식이 없거나 응급환자 또는 보호자가 없는 경우는 예외)를 받아 송부하여야 한다. 또한 응급환자를 다른 의료기관에 이송하는 경우에는 지체 없이 내원 당시 작성된 진료기록의 사본 등을 이송해야 한

다(제21조 제3항~제5항).

라. 의학연구 등 의료정보의 이차적 이용(secondary use)[35]

① 판례에 따르면, 의료법 제21조 제2항에서 열거한 법률 규정에 의한 공개 이외에 국세청 연말정산간소화서비스시스템에 따른 의료기관 수진자의 의료비 소득공제증명서류를 자료집중 기관(국민건강보험공단)에 제출하도록 한 소득세법 제165조제1항(소득공제 증명서류의 제출 및 행정지도)은 위헌이 아니라고 판결한바 있다.[36] ② 그리고 의학교육과 의학연구에 2차적으로 활용하는 것을 허용하는 법률 규정이 없는 경우에는 환자의 동의를 받아야 한다. 다만, 개인정보보호법에서는 통계작성 및 학술연구 등의 목적을 위해 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 있도록 허용하고 있다(제18조 제2항 제4호). 또한 생명윤리 및 안전에 관한 법률에 의하면 유전자은행은 수집한 모든 유전정보 등을 익명화(정보에서 개인을 파악할 수 있는 식별표지를 제거하는 것) 하여 보관·관리해야 하며(제35조의2 제1항), 이때 성명·주민등록번호·주소 등 개인 식별이 가능한 정보는 코드 또는 암호 등을 이용하여 익명화해야 한다(동법 시행규칙 제26조의2 제2항 2호). 한편, 의료기관 개인정보보호 가이드라인(보건복지부)에서는 연구와 관련되어 연구계획서 심의와 함께 개인정보를 다루는 경우에는 개인정보보호위원회가 그 권한을 의료기관내 연구윤리심의위원회(생명윤리 및 안전에 관한 법률에 의한 기관생명윤리심의위원회, 의약품 임상시험 관리기준에 의한 의약품임상시험심사위원회: IRB)에 위임할 수 있도록 규정하

---

35) 김장한, "의료기관 개인건강정보의 이차적 이용", 『의료법학』, 제11권 제1호, 대한의료법학회, 2010, 제126~134면; 김진경·한우석, "의료정보 이용 및 공개에 관한 법적 기준-미국 프라이버시규칙과 피험자보호규칙의 검토", 『한양법학』, 제20권 제4호, 한양법학회, 2009, 제215~218면 참조.

36) 헌법재판소 2008.10.30. 선고 2006헌마1401,1409병합 결정.

고 있다.[37]

마. 정보공개법에 의한 공개

행정기관의 행정정보 가운데 의료에 관련된 정보의 공개제도에 대해서는 헌법 제21조의 국민의 알권리 보장 등에 근거하는 공공기관의 정보공개에 관한 법률의 적용을 받으며, 비공개 대상 정보(제7조)를 제외하고는 공개될 수 있다. 여기서 말하는 정보란 공공기관이 직무상 작성 또는 취득하여 관리하고 있는 문서(전자문서 포함)·도면·사진·필름·테이프·슬라이드 및 이에 준하는 매체 등에 기록된 사항을 말한다. 또 행정기관에는 국가·지방자치단체와 보건복지부·국민건강보험공단·건강보험심사평가원 등이 해당되고 경우에 따라서는 국·공립 의료기관도 포함될 수 있다.

VI. 결 론

일반적으로 환자의 개인정보인 보건의료정보는 의료기관에서 진료기록부 형태로 생성되어 활용되고 보존 및 폐기되는데 의료기관뿐 아니라 기타 기관에서도 생성되고 유통되는 포괄적인 의미로 파악할 필요가 있다. 오늘날 정보통신기술이 발달함에 따라 디지털화 된 보건의료정보가 의료목적이나 그 밖에 다양한 목적으로 의료기관간 또는 개인 간에 공동 활용되는 경우가 빈번해지고 있어 그것의 유출 및 보호문제가 심각한 사회적 이슈로 떠오르고 있는 실정이다. 이러한 측면에서 환자의 개인정보는 '민감정보'에 해당하는 것으로 일반 개인정보보다 강도 높게 보호할 필요가 있게 된다.

보건의료정보를 보호하는 법적 근거는 의사의 직업윤리나 의료계약상 의무에서도 찾을 수 있지만 보다 중요한 것은 헌법상 인정되는 개인정보자기결

37) 보건복지부, 전게서, 제4면.

정권에 근거하는 기본권에 해당한다는 점에서 중요하게 다루어져야 한다. 또 실정법상으로는 민·형사법, 보건의료관련법, 정보통신 관련법 등에서 보호규정을 두고 있으나 가장 중요한 것으로는 2011.9.30일부터 시행된 개인정보보호법이며, 보건복지부에서도 의료기관 개인정보보호 가이드라인을 제정하여 2010.3.15일부터 시행하고 있다. 이 가이드라인에 따르면 기술적·물리적 보호조치와 함께 관리적 보호조치를 취하도록 하고 있으나 현재 실제로 개별 의료기관에서 개인정보보호위원회 설치, 개인정보관리책임자·개인정보보호실무책임자·개인정보보안실무책임자 각 1인 채용 또는 임명, 종사자의 직무수행 시 정보보호규정에 따른 접근권한 통제 등이 완벽하게 이루어지지 않고 있는 실정이다.

또한 법제도적 보호측면에서 의료법을 비롯한 21개 법률의 규정을 조사해 본 결과, 환자의 개인정보를 침해한 경우 각 법률마다 손해배상책임이나 형사적 벌칙조항이 다르게 규정되어 있는 것으로 파악됐다. 그 가운데 개인정보 보호의무를 위반한 경우에 대해 의료법에서는 5년 이하 징역 또는 2천만 원 이하 벌금에 처하도록 하고 있는 반면에 개인정보보호법에서는 5년 이하 징역 또는 5천만 원 이하 벌금에 처하도록 규정하고 있는바, '민감정보'에 해당하는 환자의 개인정보를 일반 개인정보보다 가볍게 처벌하도록 규정하고 있는 것은 모순이며 의료법상 벌칙규정을 상향 조정할 필요가 있다.

그리고 의료기관 및 그 종사자는 개인정보보호법에서 정하는 개인정보를 수집·이용·파기 또는 그 제한되는 경우, 환자의 동의를 받는 방법과 절차 등이 복잡하더라도 이를 철저히 준수하여 환자의 개인정보를 불법적으로 유출시키지 않도록 해야 한다. 그렇게 하기 위해서는 보건복지부의 가이드라인이 개별 의료기관에서 정확하게 시행될 수 있도록 행정지도와 보안감사를 정례적으로 실시해야 것이다. 특히, 감독기관인 보건복지부는 개별 의료기관이 개인정보보호위원회 설치, 개인정보관리책임자·개인정보보호실무책임자·개인정보보안실무책임자 각 1인 채용 또는 임명이 이루어질 수 있도록 지도감독을 강화해야 하며, 의료현장인 개별 의료기관에서는 그 종사자들이

법규 및 지침을 정확히 숙지하고 병원업무를 수행할 수 있도록 정보보호교육을 보다 실질적으로 실시할 필요가 있다.

한편, 의료법에 따른 의무기록 열람 및 사본교부는 정보주체 및 그 가족 등에 의한 환자의 개인정보 열람 및 교부제도가 법제화되어 있기 때문에 병원현장에서는 매뉴얼에 따라 지켜지고 있는 것으로 파악된다. 또한 각종 법률 규정에 의한 열람 및 교부, 환자이송 등에 따른 의료기관 간 의료정보 교환, 정보공개법에 따른 공개 등의 경우에는 실무자가 해당 법률 규정에 따라 기관 대 기관의 방식으로 관련 업무를 수행하기 때문에 크게 문제가 되지 않는 것으로 보인다. 다만, 환자의 개인정보를 의학연구나 의학교육과 같은 이차적 목적(secondary use)으로 이용하는 경우에는 그 사용자가 주로 의사나 교수 등 개인이라는 점에서 동의 없는 사용이나 환자정보 유출 등의 문제가 발생하는 경우가 있다. 또한 의약품 임상시험의 경우에는 별도 기준에 따라 피험자로 참가하는 환자를 모집하는 과정에서 동의를 받고 있지만, 그 이외에 의사나 교수 개인이 환자의 치료사례를 기본데이터로 활용해서 논문을 작성하는 경우에는 의료기관이 직접 환자동의나 개인정보 익명화 처리방법 등에 대해 그 종사자들에게 관련 법규와 지침을 제시하고 이를 준수하도록 유도하는 노력이 필요하다.

주제어 : 보건의료정보, 개인정보, 의무기록, 전자의무기록, 개인정보자기결정권, 개인정보보호법

〔 참 고 문 헌 〕

1. 국내문헌

경희의료원(정용엽 외 5인 공저), 『경희의료원20년사』, 1992.

권권보, 『개인정보보호와 자기정보통제권』, 경인문화사, 2005.

길준규, “의료정보상 개인정보보호방안-독일법과 정보보호법리를 중심으로”, 『법과 정책연구』, 제6권 제1호, 한국법정책학회, 2006. 6.

김상겸, “독일의 의료정보와 개인정보보호에 관한 연구”, 『한독사회과학논총』, 제14권 제2호, 한독사회과학회, 2005.

김성현·김민우·오암석·김관형·강성인, “u-헬스케어 시스템의 의료정보 표준화 기술에 관한 연구”, 『한국멀티미디어학회 추계학술발표대회 논문집』, 제13권 제2호, 한국멀티미디어학회, 2010.

김장한, “의료기관 개인건강정보의 이차적 이용”, 『의료법학』, 제11권 제1호, 대한의료법학회, 2010. 6.

김진경·한우석, “의료정보 이용 및 공개에 관한 법적 기준-미국 프라이버시규칙과 피험자보호규칙의 검토”, 『한양법학』, 제20권 제4호, 한양법학회, 2009. 11.

백윤철, “미국의 개인정보보호와 HIPAA”, 『미국헌법연구』, 제19권 제1호, 미국헌법학회, 2008. 2.

백윤철, “우리나라에서 의료정보와 개인정보보호”, 『헌법학연구』, 제11권 제1호, 한국헌법학회, 2005.

보건복지부, 『의료기관 개인정보보호 가이드라인(500병상 이상 의료기관 대상)』, 2010. 3.

송지은·김신효·정명애, “u-헬스케어 서비스에서의 의료정보보호”, 『정보보호학회지』, 제17권 제1호, 한국정보보호학회, 2007. 2.

윤명선, 『인터넷시대의 헌법학』, 대명출판사, 2010.

이경권, “환자 의료정보보호와 관련된 법적 쟁점”, 『한국의료QA학회지』, 제15권 제2호, 한국의료QA학회, 2009.

이백휴, “환자의 의무기록 관련 의료인의 법적 지위”, 『의료법학』, 제11권 제2호, 대한의료법학회, 2010. 12.

이부하, “환자의 의료정보권”, 『한양법학』, 제17집, 한양법학회, 2005.
이진영, “보건의료분야에서의 자기정보통제권”, 『생명윤리정책연구』, 제3권 제2호, 생명윤리정책연구센터, 2009.
일본의사회, 『진료정보제공에 관한 지침 2-1(1) (번역문)』, 2002. 10. 22.
전영주, “의료법상 의료정보 보호방안-의무기록 보호를 중심으로”, 『법학연구』, 제28집, 한국법학회, 2007. 11.
전영주, “의료정보와 개인정보보호”, 『법학연구』, 제23집, 한국법학회, 2006.8.
정부균, “환자 의료정보 보호의 문제”, 『의료법학』, 제9권 제2호, 대한의료법학회, 2008. 12.
정용엽, “u-헬스케어에 있어서 디지털의료정보의 법률적 보호”, 『국제법무연구』, 제10호, 경희대학교 국제법무대학원, 2006. 2.
정용엽, 『u-Health 시대의 원격의료법』, 한국학술정보㈜, 2008.
정혜정·김남현, “보건의료의 정보화와 정보보호관리 체계”, 『정보보호학회지』, 제19권 제1호, 한국정보보호학회, 2009. 2.
조형원, “유비쿼터스 보건의료서비스 활성화지원 법률안의 제안”, 『의료법학』, 제10권 제1호, 대한의료법학회, 2009. 6.
국민일보 쿠키뉴스, “보건연, 6개 병원 2000여 명 환자정보 유출”, 9. 29. 2011 (http://news.kukinews.com/).
뉴시스, “휴·폐업중인 병원 진료기록부 발급 쉬워진다”, 12. 6. 2012 (www.newsis.com/).
데일리메디, “의협, 유비케어 자료획득 자체가 위법”, 11. 8. 2011 (www.dailymedi.com/).
디지털데일리, “의협 vs 유비케어, 개인정보유출 논란 법정으로”, 11. 8. 2010 (www.ddaily.co.kr/).
연합뉴스, “박원순 아들 세브란스병원서 MRI 촬영”, 2. 22. 2012(www.yonhapnews.co.kr/)
전자신문, “중소 병·의원들 개인정보 불감증 치료부터…”, 3. 19. 2012 (www.etnews.com/).

2. 외국문헌

Health Insurance Portability and Accountability Act(HIPAA) Ⅱ-F(Administrative Simplification) (1996).

ILO Code of Practice on the Protection of Worker's Personal Data (1997).

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

The Protection of Individuals with regard to the Procession of Personal Data and on the Free Movement of such Data(EU) (1995).

UN Guidelines Concerning Computerized Personal Data Files (1990).

A Study on Legal Protection, Inspection and Delivery of the Copies of Health & Medical Data

Yong-Yeub, Jeong

KyungHee University Medical Center

=ABSTRACT=

In a broad term, health and medical data means all patient information that has been generated or circulated in government health and medical policies, such as medical research and public health, and all sorts of health and medical fields as well as patients' personal data, referred as medical data (filled out as medical record forms) by medical institutions. The kinds of health and medical data in medical records are prescribed by Articles on required medical data and the terms of recordkeeping in the Enforcement Decree of the Medical Service Act.

As EMR, OCS, LIS, telemedicine and u-health emerges, sharing and protecting digital health and medical data is at issue in these days. At medical institutions, health and medical data, such as medical records, is classified as "sensitive information" and thus is protected strictly. However, due to the circulative property of information, health and medical data can be public as well as being private. The legal grounds of health and medical data as such are based on the right to informational self-determination, which is one of the fundamental rights derived from the Constitution. In there, patients' rights to refuse the collection of information, to control recordkeeping (to demand access, correction or deletion) and to control using and sharing of information are rooted.

In any processing of health and medical data, such as generating, recording, storing, using or disposing, privacy can be violated in many ways, including the leakage, forgery, falsification or abuse of information. That is why laws,

such as the Medical Service Act and the Personal Data Protection Law, and the Guideline for Protection of Personal Data at Medical Institutions (by the Ministry of Health and Welfare) provide for technical, physical, administrative and legal safeguards on those who handle personal data (health and medical information-processing personnel and medical institutions). The Personal Data Protection Law provides for the collection, use and sharing of personal data, and the regulation thereon, the disposal of information, the means of receiving consent, and the regulation of processing of personal data.

On the contrary, health and medical data can be inspected or delivered of the copies, based on the principle of restriction on fundamental rights prescribed by the Constitution. For instance, Article 21(Access to Record) of the Medical Service Act, and the Personal Data Protection Law prescribe self-disclosure, the release of information by family members or by laws, the exchange of medical data due to patient transfer, the secondary use of medical data, such as medical research, and the release of information and the release of information required by the Personal Data Protection Law.

Keyword : Health & Medical Data, Personal Data. Medical Record, Electronic Medical Record (EMR), the Right to Informational Self-Determination, the Personal Data Protection Law