대한의료법학회
『의료법학』 제21권 제2호
https://doi.org/10.29291/kslm.2020.21.2.075

의료법의 개인정보보호에 관한 연구

성 수 연*

I. 들어가며

정보통신기술의 발전은 의료환경에도 큰 영향을 미쳐 의료전달체계인 OCS[1], EMR[2], EDI[3]을 이용한 전자청구시스템 등의 도입을 가속화시켰다. 이로 인해

* 논문접수: 2020. 9. 11. * 심사개시: 2020. 9. 14. * 게재확정: 2020. 9. 21.
* 단국대학교 보건행정학과 강사, 고려대학교 법학연구원. (sooyeanii@naver.com).

1) Ordering Communication System, 처방전달시스템이란 의료 기관에서 컴퓨터망을 통해 의사의 처방을 각종 진료 지원부에 전달함으로써 진료 및 처방에 소요되는 시간을 대폭 줄이고, 처방 내역을 컴퓨터에 저장해 두고 환자 진단 시에 이를 손쉽게 조회할 수 있어 진료의 질을 높일 수 있는 의료 정보 시스템.
https://terms.naver.com/entry.nhn?docId=3435643&cid=42346&categoryId=42346.

2) Electronic Medical Record, 전자의무기록이란 의사가 직접 컴퓨터에 환자의 임상진료에 관한 모든 정보를 입력하면 이 자료를 모두 데이터베이스로 처리, 새로운 정보의 생성도 가능한 의료정보시스템으로 HIS(Hospital Information System, 병원정보시스템)의 일부분이다. 이 시스템은 소프트웨어와 진료실PC*접수실PC*프린터*서버*허브*검사실PC 등 하드웨어로 구성돼 있으며 이를 통해 일일이 수작업으로 종이에 환자기록을 정리 하는 방식보다 의료기관의 업무를 대폭 줄일 수 있다. 특히 환자의 진료기록을 찾아서 진료실에 전달하고 다시 처방전을 받아 조제하는 일련의 과정이 컴퓨터 네트워크를 이용해 처리함으로써 환자

환자는 신속하게 진료 및 처방을 받고, 의료인과 환자의 편의는 증대되었다.

이러한 의료정보화는 환자의 기본인적 정보와 고유식별정보, 의료건강정보, 경제정보, 바이오정보 등 개인정보를 다양하게 수집·이용하는 등 개인정보 처리[4]를 용이하게 하였으며, 이를 의료의 질 향상과 맞춤 의료서비스의 제공 등에 활용하고 있다.

그러나 개인정보 유출로 인한 사적 비밀의 침해와 위·변조로 인한 정보의 완전성이 침해될 위험성이 생기게 되었다. 최근 미국 시카고대학 의대와 제휴된 대형 병원 시스템의 환자 등 35만 명의 개인정보가 해킹을 당해 대량으로 유출[5]되었고, 국내 한 종합병원 건강검진 의사가 SNS로 환자에게 마음에 든다는 메시지를 보내[6]기도 하였다. 국민건강보험공단 직원 징계 내역(2014년~2017년 7월 말)에 따르면 징계를 받은 직원 총 74명 중 15명이 개인정보 무단열람 등 개인정보를 부적절하게 처리한 혐의로 징계를 받은 것[7]으로 드러났다.

개인정보 유출 등으로 인해 사회적 낙인 또는 배제, 비급여의 증가, 의료인과의 불신 등 개인적 피해와 의료기관 및 건강보험공단의 신뢰 저하, 수입 감소 등은 사회적 문제로 대두될 수 있다.

정보화 시대에 발맞추어 환자의 사생활 보호와 알 권리 보장, 개인정보자기

대기시간이 줄어들고 별도의 진료기록실이 불필요하다.
https://terms.naver.com/entry.nhn?docId=2075181&cid=42107&categoryId=42107.

3) Electronic Data Interchange. 전자자료 교환방식이란 거래당사자 간에 사람이나 우편에 의하여 전달되는 종이문서 대신 컴퓨터가 인식할 수 있는 서로 합의된 표준화된 자료(전자문서)를 데이터 통신망을 통해 컴퓨터와 컴퓨터 간에 교환하여 재입력 과정 없이 직접 업무에 활용할 수 있도록 하는 정보 전달 방식.
https://edi.nhis.or.kr/homeapp/wep/f/retrieveFaq.do.

4) 개인정보보호법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
2. "처리"란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

5) SBS, "미 시카고의대 제휴 대형 병원시스템서 35만 명 개인정보 유출", 2020. 09. 10.
https://news.sbs.co.kr/news/endPage.do?news_id=N1005973542&plink=ORI&cooper=NAVER&plink=COPYPASTE&cooper=SBSNEWSEND.

6) MBC, "건강검진 환자에 "느낌 좋다" 문자…의사 해고", 2020. 08. 31.
https://imnews.imbc.com/replay/2020/nwtoday/article/5893180_32531.html.

7) 의협신문, "건보공단 직원, 환자 개인 의료정보 유출", 2017. 10. 23.
http://www.doctorsnews.co.kr/news/articleView.html?idxno=119370.

결정권을 보호하고 침해를 예방하기 위한 「개인정보 보호법」과 가이드라인[8] 등이 있으나 국민의료에 관한 전반적인 사항을 규정한 「의료법」에서는 정보 누설 금지와 기록 열람 등 제한, 전자처방전·전자의무기록·진료기록전송지원시스템의 개인정보 유출 금지 등을 규정하고 있을 뿐 민감정보인 의료건강정보를 포함한 환자의 개인정보를 보호하기에는 미흡한 실정이다.

의료법은 개별 조항에서 정보와 개인정보, 진료정보 등 용어를 혼용하고 있는데 구체적으로 객체인 개인정보를 명확하게 할 필요가 있으며, 제23조제3항의 경우 "누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하는 경우를 금지"하고 있는데 이를 예시규정으로 보아야 하는지 앞서 본 행위만을 금지하는 열거규정으로 보아야 하는지 판단할 필요가 있다. 대법원은 "의료인은 전자의무기록에 대하여 변조행위의 주체가 될 수 없다"[9]고 하여 주체에 따라 불법행위를 명확히 규정할 필요가 있다.

이번 연구에서는 위와 같은 필요성을 바탕으로 개인정보에 관한 일반법인 개인정보보호법과 환자의 개인정보에 관한 특별법인 의료법을 비교하여 동일한 사항을 달리 규정하고 있는 경우에는 특별법인 의료법을 우선 적용한다는 점을 적용하여 환자의 개인정보에 대한 정의와 적용범위, 개인정보 처리에서 발생하는 불법행위 및 주체를 명확히 하고, 벌칙에 차이를 두고 있는 의료법의 타당성을 검토하고자 한다.

II. 의료기관의 개인정보 처리

1. 개인정보보호법의 개인정보

개인정보보호법 제2조에서 개인정보를 "살아있는 개인에 관한 정보"로서

---

8) 보건복지부 및 행정안전부, 「개인정보 보호 가이드라인-의료기관편」, 2015. 2.
9) 대법원 2011. 6. 30. 선고 2011노317 판결.

제2조제1호가목 “성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보”로 규정하고 있으며, 제2조제1호나목은 “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보”로 규정하면서 “이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.”라고 설명하고 있다. 마지막으로 제2조제1호다목에서 “가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다)”라고 정의하고 있다.

개인정보의 구성요소로 가. ‘살아 있는 개인’, 나. ‘특정 개인과의 관련성’, 다. ‘정보의 종류·형태 비제한 및 식별가능성’이 있다. 이하에서는 개인정보의 구성요소에 대해 개별적으로 살펴본다.

가. 살아있는 개인

개인정보보호법에 따른 개인정보는 “현재 ‘생존(生存)하고 있는 개인(자연인)’에 관한 정보에 한정한다. 따라서, 이미 사망하였거나 실종선고 등 관계 법령에 의해 사망한 것으로 간주 되는 자, 법인(法人)이나 단체에 관한 정보는 개인정보로 볼 수 없다. 사자의 정보가 배제되는 이유는 개인정보의 보호법익은 프라이버시권(사생활의 비밀과 자유)인 ‘인격권’으로서 상속이 불가능하고 사망자의 정보에 대해 권리를 행사할 주체가 존재하지 않게 되므로, 보호대상이 되는 개인정보의 주체를 생존하는 개인으로 한정한 것이다. 다만, 사망자의 정보가 사망자와 유족과의 관계를 나타내는 정보이거나 유족 등의 사생활을 침해하는 등의 경우에는 사망자 정보인 동시에 관계되는 유족의 정보”[10]이기도 하므로 개인정보보호법에 따른 보호대상이 될 수 있다.

---

10) 행정안전부, 「개인정보 보호법령 및 지침·고시 해설」, 2011. 12, 6면.

나. 특정 개인과의 관련성

제2조제1호나목에서의 "특정 개인은 일반적으로 특정 개인의 정체성(identity)을 구별하거나 밝혀낼 수 있는 정보(성명, 주민등록번호, 생일, 주소, 바이오정보 등)와 특정 개인의 과거와 현재의 상황이나 상태를 나타낼 수 있는 정보(교육상황, 재정상황, 진료 및 건강 상태 등)가 이에 해당하며 특정 개인을 알아볼 수 없도록 가명·익명처리 되었거나 특정 단체 임원들의 평균연봉, 특정 대학의 해당연도 졸업생의 취업률 등 통계적으로 변환된 경우에는 특정 개인과의 관련성이 없고 식별이 어려워 개인정보에 해당하지 않는다."[11]

다. 정보의 종류·형태 비제한 및 식별가능성

개인정보보호법에서의 개인정보는 "개인을 알아볼 수 있는 정보 또는 추가정보의 사용결합 없이는 특정 개인을 알아볼 수 없는 정보라고 규정하고 있을 뿐 정보의 종류, 성격, 형식 등에 대해서는 특별한 제한을 두고 있지 않다.

객관적인 정보인 개인의 신장, 체중, 나이와 직장에서의 근무 평가, 금융기관의 개인 신용도 등은 주관적 정보로 개인정보에 해당될 수 있다. 이러한 정보는 허위이거나 정확성이 떨어지는 정보이더라도 개인과 관련된 정보이면 개인정보가 될 수 있다.

개인정보는 컴퓨터 등에 저장된 문서, 파일의 전자기적 형태, 종이문서의 수기 형태, 녹음된 음성정보, 영상정보처리기기에 녹화된 영상, 기타 문자, 부호, 그림, 숫자, 사진, 그래픽, 이미지, 음성, 음향, 형상 등의 형태로 처리된 정보 모두를 포함한다. 이러한 개인정보는 종류, 형태, 성격 등 별도의 규정이 없더라도 특정 개인과 다른 사람을 구분하거나 구별할 수 있는 정보이어야 한다. 예를 들어 주민등록번호, 여권번호, 운전면허의 면허번호 등 고유식별정보와 성명, 주소, 본적 등 인적 정보, 학생의 학번, 회사 사번, 가입한 기업의 ID 등이 특정 개인을 식별할 수 있는 정보가 된다.

---

11) 행정안전부, 위의 책, 7면.

이 외에도 제2조제1호나목의 다른 정보와 쉽게 결합하여 특정개인을 알아볼 수 있는 정보도 개인정보로 규정하고 있다. 여기서의 쉽게 결합할 수 있는지의 여부는 다른 정보의 입수가능성 등 개인을 알아보는데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다"[12]는 의미로 불합리할 정보의 시간, 노력, 비용이 투입된다면 식별 가능성이 없다고 보아야 할 것이다.

2. 의료기관의 개인정보 처리

개인정보는 일반정보, 신체적 정보, 정신적 정보, 재산적 정보, 사회적 정보 등으로 구분[13]할 수 있다. 성명, 주민등록번호, 주소, 전화번호, 생년월일, 이메일 주소, 가족관계 및 가족 구성원의 정보 등이 일반정보에 포함되며, 신체적 정보 중 건강상태, 진료기록, 신체장애, 장애등급은 의료건강정보에 해당하며, 얼굴, 지문, 음성, 유전자 정보, 키, 몸무게는 신체 정보에 포함된다. 도서·비디오 대여기록, 신문·잡지 구독 정보, 인터넷 검색 내역, 종교 및 활동 내역, 정당·노조 가입 여부 및 활동 내역은 정신적 정보에 해당하고, 소득정보, 신용카드 번호 및 비밀번호, 통장계좌번호 및 비밀번호, 개인신용평가정보 등은 재산적 정보에 속한다. 학력, 성적, 출석상황, 전과·범죄 기록, 재판기록, 직장, 근무처, 근로경력 등은 사회적 정보에 해당한다.

의료기관에서 생성, 이용되는 환자의 개인정보는 의료행위 과정에 필요한 환자의 인적 정보인 성명, 주민등록번호, 연락처, 환자등록번호, 진료카드번호, 건강보험증번호, 아이디, 비밀번호 등과 의학적 배경정보인 유전자 정보, 환자의 건강상태, 신체적 특징, 병력(가족력), 체력, 유전정보, 신용카드정보 등이 있다.

이러한 환자의 개인정보는 의료건강정보 외에 여러 정보를 포함하고 있어 가장 민감한 정보로서 높은 수준의 보호조치가 필요한 정보 중 하나에 속한다. 보호되는 정보에는 정보시스템에 저장된 정보뿐만 아니라 모든 유형의 개인정보를 포함

12) 행정안전부, 위의 책, 8-9면.
13) 보건복지부 및 행정안전부, 위의 책, 44면.

하고 있어 종이문서 또는 구두로 전달되는 정보까지 보호대상으로 하고 있다.

III. 의료법에 규정된 개인정보

1. 의료법에서의 개인정보

의료기관에서 처리되는 환자의 개인정보의 종류, 성격, 형식 등에 대하여 의료법에 특별한 규정을 두고 있지 않으며, 「보건의료기본법」에서 보건의료정보에 관련하여 정의하고 있다. 제3조제1호는 보건의료에 관하여 "국민의 건강을 보호·증진하기 위하여 국가·지방자치단체·보건의료기관 또는 보건의료인 등이 행하는 모든 활동"이라고 정의하면서 "보건의료와 관련한 지식 또는 부호, 숫자, 문자, 음성, 음향, 영상 등으로 표현된 모든 종류의 자료"를 보건의료정보라고 규정하고 있다. 이를 의료법에 적용하면, 의료기관이나 의료인이 행하는 모든 활동에 관한 지식, 부호, 숫자, 문자, 음성, 음향 등으로 표현된 모든 자료를 말하며, 의료법의 적용을 받는 진료기록부, 간호기록부, 조산기록부, 처방전, 진단서 등에 작성·보관된 정보를 말한다.

구체적으로 환자의 개인정보를 '주관적 정보', '객관적 정보', '가치판단정보'로 구분[14]할 수 있다. '주관적 정보'에는 진료기록부, 조산기록부에 기록하여야 하는 인적사항으로 진료를 받은 사람의 주소, 성명, 연락처, 주민등록번호 등[15]이 이에 해당하며, 환자에 의하여 작성된다. '객관적 정보'에는 진료기록

---

14) 조홍석, "위험사회에 있어 개인의 의료정보 보호방안", 한양법학(제24권 4집), 한양법학연구소, 2013. 11, 174면.

15) 의료법 시행규칙 제14조(진료기록부 등의 기재 사항) ① 법 제22조제1항에 따라 진료기록부·조산기록부와 간호기록부(이하 "진료기록부등"이라 한다)에 기록해야 할 의료행위에 관한 사항과 의견은 다음 각 호와 같다. <개정 2013. 10. 4.>.
1. 진료기록부
가. 진료를 받은 사람의 주소·성명·연락처·주민등록번호 등 인적사항
나. 주된 증상. 이 경우 의사가 필요하다고 인정하면 주된 증상과 관련한 병력(病歷)·가족력(家族歷)을 추가로 기록할 수 있다.
다. 진단결과 또는 진단명

부의 기재 사항인 주된 증상, 치료 내용, 진료 일시 및 간호기록부의 체온·맥박·호흡·혈압에 관한 사항, 간호 일시 등이 해당되며, 조산기록부의 생·사산별 분만 횟수, 임신 중의 의사에 의한 건강진단의 유무, 분만 장소 및 분만 연월시분 등[16]이 포함된다. '가치판단정보'는 의료인의 전문성에 기인한 정보로서 진료기록부의 진단결과 또는 진단명, 조산기록부의 임신 후의 경과와 그에 대한 소견, 산아와 태아부속물에 대한 소견 등이 이에 해당된다.

진료기록부 등에 기록·저장된 정보가 환자의 개인정보로서 보호받기 위하여는 개인정보보호법에 따라 특정개인을 식별할 수 있는 정보이어야 한다. 인적사항과 고유식별정보는 식별가능성이 있어 당연히 환자의 개인정보에 해당할 수 있고, 환자의 주된 증상, 진단 결과, 체온·맥박·호흡·혈압에 관한 사항 등은 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 경우에 개인정보에 포함될 수 있다.

라. 진료경과(외래환자는 재진환자로서 증상·상태, 치료내용이 변동되어 의사가 그 변동을 기록할 필요가 있다고 인정하는 환자만 해당한다)
마. 치료 내용(주사·투약·처치 등)
바. 진료 일시(日時)

16) 의료법 시행규칙 제14조(진료기록부 등의 기재사항)
2. 조산기록부
가. 조산을 받은 자의 주소·성명·연락처·주민등록번호 등 인적사항
나. 생·사산별(生·死産別) 분만 횟수
다. 임신 후의 경과와 그에 대한 소견
라. 임신 중 의사에 의한 건강진단의 유무(결핵·성병에 관한 검사를 포함한다)
마. 분만 장소 및 분만 연월일시분(年月日時分)
바. 분만의 경과 및 그 처치
사. 산아(産兒) 수와 그 성별 및 생·사의 구별
아. 산아와 태아부속물에 대한 소견
자. 삭제 <2013. 10. 4.>
차. 산후의 의사의 건강진단 유무
3. 간호기록부
가. 간호를 받는 사람의 성명
나. 체온·맥박·호흡·혈압에 관한 사항
다. 투약에 관한 사항
라. 섭취 및 배설물에 관한 사항
마. 처치와 간호에 관한 사항
바. 간호 일시(日時)

2. 개인정보 관련 규정

의료법에서의 환자 개인정보에 관한 규정으로 제19조 정보 누설 금지[17], 제21조의2 진료기록의 송부 등[18], 제23조 전자의무기록[19], 제23조의3 진료정보 침해사고의 통지[20], 제23조의4 진료정보 침해사고의 예방 및 대응 등[21]

---

17) 의료법 제19조(정보 누설 금지) ① 의료인이나 의료기관 종사자는 이 법이나 다른 법령에 특별히 규정된 경우 외에는 의료·조산 또는 간호업무나 제17조에 따른 진단서·검안서·증명서 작성·교부 업무, 제18조에 따른 처방전 작성·교부 업무, 제21조에 따른 진료기록 열람·사본 교부 업무, 제22조제2항에 따른 진료기록부등 보존 업무 및 제23조에 따른 전자의무기록 작성·보관·관리 업무를 하면서 알게 된 다른 사람의 정보를 누설하거나 발표하지 못한다. <개정 2016. 5. 29.>
② 제58조제2항에 따라 의료기관 인증에 관한 업무에 종사하는 자 또는 종사하였던 자는 그 업무를 하면서 알게 된 정보를 다른 사람에게 누설하거나 부당한 목적으로 사용하여서는 아니 된다. <신설 2016. 5. 29.> [제목개정 2016. 5. 29.]

18) 의료법 제21조의2(진료기록의 송부 등) ① 의료인 또는 의료기관의 장은 다른 의료인 또는 의료기관의 장으로부터 제22조 또는 제23조에 따른 진료기록의 내용 확인이나 진료기록의 사본 및 환자의 진료경과에 대한 소견 등을 송부 또는 전송할 것을 요청받은 경우 해당 환자나 환자 보호자의 동의를 받아 그 요청에 응하여야 한다. 다만, 해당 환자의 의식이 없거나 응급환자인 경우 또는 환자의 보호자가 없어 동의를 받을 수 없는 경우에는 환자나 환자 보호자의 동의 없이 송부 또는 전송할 수 있다.
⑧ 누구든지 정당한 사유 없이 진료기록전송지원시스템에 저장된 정보를 누출·변조 또는 훼손하여서는 아니 된다.
⑨ 진료기록전송지원시스템의 구축·운영에 관하여 이 법에서 규정된 것을 제외하고는 「개인정보 보호법」에 따른다.
[본조신설 2016. 12. 20.]

19) 의료법 제23조(전자의무기록) ③ 누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.

20) 의료법 제23조의3(진료정보 침해사고의 통지) ① 의료인 또는 의료기관 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등 대통령령으로 정하는 사고(이하 "진료정보 침해사고"라 한다)가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하여야 한다.
② 보건복지부장관은 제1항에 따라 진료정보 침해사고의 통지를 받거나 진료정보 침해사고가 발생한 사실을 알게 되면 이를 관계 행정기관에 통보하여야 한다. [본조신설 2019. 8. 27.]

21) 의료법 제23조의4(진료정보 침해사고의 예방 및 대응 등) ① 보건복지부장관은 진료정보 침해사고의 예방 및 대응을 위하여 다음 각 호의 업무를 수행한다.
1. 진료정보 침해사고에 관한 정보의 수집·전파
2. 진료정보 침해사고의 예보·경보
3. 진료정보 침해사고에 대한 긴급조치
4. 전자의무기록에 대한 전자적 침해행위의 탐지·분석
5. 그 밖에 진료정보 침해사고 예방 및 대응을 위하여 대통령령으로 정하는 사항

이 있다. 의료법 제19조제1항은 의료인이나 의료기관 종사자가 관련 업무에 종사하면서 알게 된 “정보”를, 제21조의2제8항은 진료기록전송지원시스템에 저장된 “정보”를, 제23조제3항은 전자의무기록에 저장된 “개인정보”를, 제23조의3 및 제23조의4는 전자의무기록에 저장된 “진료정보”를 누설, 유출, 변조, 훼손 등 행위를 금지하고 있으며, 보호주체에 대한 용어를 각 조항에서 다르게 사용하고 있다.

가. 의료법 제19조 정보 누설 금지

의료법 제19조는 의료인이나 의료기관 종사자가 의료행위에 있어 지득한 환자 등의 정보를 누설함을 금지함으로써 정확하고 적절한 진료를 위한 전제가 되는 신뢰관계를 보호하기 위하여 의료인이 의료행위 과정에서 알게 된 정보를 누설하지 않을 직업윤리를 의무화하여 법률로 규정한 것[22]으로 의료인 등이 업무와 관련하여 알게 된 정보에 대해서는 구체적으로 규정하고 있지 않다. 이에 대법원은 “구 의료법(2016. 5. 29. 법률 제14220호로 개정되기 전의 것, 이하 ‘구 의료법’이라 한다) 제19조는 의료인의 의무 중 하나로 비밀누설 금지의무를 정하고 있다. 이는 의학적 전문지식을 기초로 사람의 생명, 신체나 공중위생에 위해를 발생시킬 우려가 있는 의료행위를 하는 의료인에 대하여 법이 정한 엄격한 자격요건과 함께 의료과정에서 알게 된 다른 사람의 비밀을 누설하거나 발표하지 못한다는 법적 의무를 부과한 것이다. 그 취지는 의료인과 환자 사이의 신뢰관계 형성과 함께 이에 대한 국민의 의료인에 대한 신뢰를 높임으로써 수준 높은 의료행위를 통하여 국민의 건강을 보호하고 증진하는 데 있다. 따라서 의료인의 비밀누설 금지의무는 개인의 비밀을 보호하는 것뿐만 아니라 비밀유지에 관한 공중의 신뢰라는 공공의 이익도 보호하고 있다고 보아야 한다. 이러한 관점에서 보면, 의료인과 환자 사이에 형성된 신뢰관계와

22) 김한나·이얼·김계현·이정찬·이평수, “개인의료정보의 관리 및 보호”, 대한의사협회정책연구소 연구보고서, 2013. 12, 44면.

이에 기초한 의료인의 비밀누설 금지의무는 환자가 사망한 후에도 그 본질적인 내용이 변한다고 볼 수 없다. 구 의료법 제19조에서 누설을 금지하고 있는 '다른 사람의 비밀'은 당사자의 동의 없이는 원칙적으로 공개되어서는 안 되는 비밀영역으로 보호되어야 한다. 이러한 보호의 필요성은 환자가 나중에 사망하더라도 소멸하지 않는다. 구 의료법 제21조제1항은 환자가 사망하였는지를 묻지 않고 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 사본을 내주는 등 내용을 확인할 수 있게 해서는 안 된다고 정하고 있는데, 이 점을 보더라도 환자가 사망했다고 해서 보호 범위에서 제외된다고 볼 수 없다.[23]"라고 판시하여 구 의료법 비밀 누설 금지에 대한 입법 취지와 다른 사람의 비밀 및 사망한 자의 비밀도 보호 대상으로 보고 있다.

개정 전 제19조는 의료·조산 또는 간호를 하면서 알게 된 다른 사람의 비밀을 규정하였으나 제17조에 따른 진단서·검안서·증명서 작성·교부 업무, 제18조 처방전 작성·교부 등 의료행위 및 기록 열람 등에서 수집·이용·제공되는 정보를 추가하였으며 비밀에서 "정보"로 개정되었다.

제19조의 정보는 개인정보보호법 제15조에 따른 당사자의 동의 또는 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 등이 아니면 원칙적으로 공개되어서는 안 되는 비밀 영역에 속하는 정보를 말한다.

비밀에 대하여 형법은 제316조 비밀침해죄[24]와 제317조 업무상비밀누설죄[25]에서 규정하고 있다. 형법에서의 "비밀"은 일반적으로 알려져 있지 않은

---

23) 대법원 2018. 5. 11. 선고 2018도2844 판결.

24) 형법 제316조(비밀침해) ① 봉함 기타 비밀장치한 사람의 편지, 문서 또는 도화를 개봉한 자는 3년 이하의 징역이나 금고 또는 500만 원 이하의 벌금에 처한다. <개정 1995. 12. 29.>.
② 봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다. <신설 1995. 12. 29.>.

25) 형법 제317조(업무상비밀누설) ① 의사, 한의사, 치과의사, 약제사, 약종상, 조산사, 변호사, 변리사, 공인회계사, 공증인, 대서업자나 그 직무상 보조자 또는 차등의 직에 있던 자가 그 직무처리중 지득한 타인의 비밀을 누설한 때에는 3년 이하의 징역이나 금고, 10년 이하의 자격정지 또는 700만원 이하의 벌금에 처한다. <개정 1995. 12. 29., 1997. 12. 13.>.
② 종교의 직에 있는 자 또는 있던 자가 그 직무상 지득한 사람의 비밀을 누설한 때에도 전항의 형과 같다.

사실로서 타인에게 알리지 않는 것이 본인에게 이익이 되는 것으로 공지의 사실은 비밀이 아니며, 개인의 비밀이 보호법익이다.[26] 그러나 일반적으로 개인정보는 개인의 내밀한 영역이나 사회영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 정보도 개인정보에 포함된다.[27] 개인정보보호법이나 의료법의 개인정보는 개인 식별이 가능한 정보로서 개인정보 자기결정권을 보호법익으로 한다. 따라서 의료법 제19조 비밀에서 "정보"로 개정된 이유는 한정된 의료·조산·간호 업무에서 알게 된 비밀 외에 앞서 살펴본 업무 등 폭넓은 정보를 보호하기 위함인데 개정 전 친고죄 규정을 두어 개인의 비밀을 보호법익으로 보고 있다.

"업무상 알게 된 개인정보"는 넓게 업무를 처리하는 과정에서 우연히 알게 된 것으로 충분하고 반드시 자신에게 부여된 업무를 처리하는 과정에서 적법하게 알게 된 것이어야 할 필요는 없다.[28] 의료인이 의료행위 과정에서 알게 된 환자에 관한 일체의 정보로서 그 범위를 어디까지 하여야 하는가는 구체적으로 파악하여야 할 것이다. 환자의 내원 사실, 치료비 등 다른 사람이 아는 것을 바라지 않는다면 개인정보자기결정권의 침해로서 의료인과 환자의 신뢰관계를 법적으로 담보하기 위하여 폭넓게 인정[29]하여야 할 것이다.

또한 개인정보에 관한 일반법인 개인정보보호법은 "살아있는 개인에 관한 정보"를, 「형법」제317조 "업무상 비밀누설죄"에서의 비밀은 "살아있는 개인에 관한 비밀"로서, 의료건강정보 등에 관한 특별법인 의료법은 사망한 후에도 비밀보호의 필요성이 소멸되지 않는다고 판시하여 살아있는 환자의 개인정보와 사망한 자의 의료건강정보 등도 보호대상이 된다.

---

26) 배종대, 『형법각칙』, 홍문사 제10전정판, 2018, 229-230면.
27) 헌법재판소 2005. 5. 26. 99헌마513.
28) 행정안전부, 위의 책, 359면.
29) 의료정책연구소, 『의료정보의 보호와 관리방안』, 2012. 4. 22면.

나. 의료법 제23조제3항 전자의무기록에 저장된 개인정보

의료인은 환자의 주된 증상, 진단 및 치료 내용 등을 진료기록부, 조산기록부, 간호기록부 등 의무기록을 갖추어 의료행위에 관한 사항과 의견을 상세히 기록하고 서명[30]하여야 한다. 진료에 관한 사항 등은 의료법 제22조에 따라 종이형태의 문서에 수기로 작성·보관하여야 하지만 진료기록부등을 전자서명이 기재된 전자문서(전자의무기록)로 작성·보관할 수 있다. 이는 작성된 내용이 어떤 형태의 문서에 보관되었는지의 차이만 있을 뿐 환자에 관한 의료건강정보는 상세히 기록하고 이를 안전하게 보관하여야 하며, 의료법 제19조에 따라 누설 등을 하여서는 아니 된다.

제23조제3항은 전자의무기록에 저장된 개인정보를 정당한 사유 없이 탐지, 누출·변조 또는 훼손하는 것을 금지하고 있다. 그러나 법률에 개인정보의 정의나 포섭의 구체적인 범위가 명확히 규정되어 있지 않아 대법원은 "그 용어가 사용된 법령 조항의 해석은 그 법령의 전반적인 체계와 취지·목적, 당해 조항의 규정 형식과 내용 및 관련 법령을 종합적으로 고려하여 해석하여야 한다. 이러한 법리를 「의료법」의 개정 연혁, 내용 및 취지, 「의료법」 제22조제1항, 제3항, 제23조제1항, 제3항, 구 「의료법 (2011. 4. 7. 법률 제10565호로 개정되기 전의 것)」 제66조제1항제3호, 「의료법 시행규칙」 제14조제1항제1호, 제3호의 규정, 의무기록에 기재된 정보와 사생활의 비밀 및 자유와의 관계 등에 비추

---

30) 의료법 5/제22조(진료기록부 등) ① 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)을 갖추어 두고 환자의 주된 증상, 진단 및 치료 내용 등 보건복지부령으로 정하는 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다. <개정 2013. 4. 5.>.
② 의료인이나 의료기관 개설자는 진료기록부등[제23조제1항에 따른 전자의무기록(電子醫務記錄)을 포함하며, 추가기재·수정된 경우 추가기재·수정된 진료기록부등 및 추가기재·수정 전의 원본을 모두 포함한다. 이하 같다]을 보건복지부령으로 정하는 바에 따라 보존하여야 한다. <개정 2008. 2. 29., 2010. 1. 18., 2018. 3. 27.>.
③ 의료인은 진료기록부등을 거짓으로 작성하거나 고의로 사실과 다르게 추가기재·수정하여서는 아니 된다. <신설 2011. 4. 7.>.
④ 보건복지부장관은 의료인이 진료기록부등에 기록하는 질병명, 검사명, 약제명 등 의학용어와 진료기록부등의 서식 및 세부내용에 관한 표준을 마련하여 고시하고 의료인 또는 의료기관 개설자에게 그 준수를 권고할 수 있다. <신설 2019. 8. 27.>.

어 보면, 「의료법」 제23조제3항의 적용 대상이 되는 전자의무기록에 저장된 '개인정보'에는 환자의 이름·주소·주민등록번호 등과 같은 '개인식별정보'뿐만 아니라 환자에 대한 진단·치료·처방 등과 같이 공개로 인하여 개인의 건강과 관련된 내밀한 사항 등이 알려지게 되고, 그 결과 인격적·정신적 내면생활에 지장을 초래하거나 자유로운 사생활을 영위할 수 없게 될 위험성이 있는 의료내용에 관한 정보도 포함된다고 새기는 것이 타당하므로 「의료법」 제23조제3항에서 정한 개인정보가 개인식별정보에 한정됨을 전제로 판단한 원심의 판단은 부적절하다."[31]고 판시하였다.

전자의무기록에 저장된 개인정보는 의료법 제19조에서의 정보와 마찬가지로 환자의 인적사항은 물론 의료건강정보 및 사회적 정보 등을 내포하며 이를 의료기관 및 의료인은 이를 안전하게 보관·관리하여야 할 의무를 진다.

다. 의료법 제23조의3 및 제23조의4 진료정보 침해사고의 통지, 예방 및 대응 등

의료법은 제23조의3 및 제23조의4를 신설하여 의료기관에서 진료기록부 등이 전자문서로 관리되고 있는 상황에서 해킹·악성코드 등 전자적 침해사고가 발생하는 경우 큰 피해가 발생할 수 있는바, 의료인 또는 의료기관의 개설자는 전자의무기록에 대한 전자적 침해행위로 진료정보가 유출되거나 의료기관의 업무가 교란·마비되는 등의 사고가 발생한 때에는 보건복지부장관에게 즉시 그 사실을 통지하도록 하고, 이러한 피해를 예방하기 위하여 진료정보 침해사고 예방 및 대응 등에 필요한 사항을 정하였다.[32]

제23조의3 및 제23조의4는 침해의 주체와 범위를 '진료정보'로 규정하고 있어 앞서 살펴본 제19조의 '정보' 및 제23조의 '개인정보'와 비교하여 포섭되는 정보의 범위를 구체적으로 밝힐 필요가 있다.

---

31) 대법원 2013. 12. 12. 선고 2011도9538 판결.
32) 법제처, 「의료법」 법률 제16555호, 2019. 8. 27, 일부개정, 시행 2019. 8. 27.

진료정보에 대하여 건강보험심사평가원은 “정보주체(요양급여비용명세서에 나타난 사람)에 대한 요양급여비용명세서에 있는 내용”[33]이라고 정의하고 있다. 요양급여비용명세서는 요양기관[34](의료기관, 약국 등)이 진찰·검사, 약제·치료재료의 지급, 처치·수술 및 그 밖의 치료 등 요양급여[35]를 한 후 본인일부부담금[36]을 제외한 요양급여비용을 국민건강보험공단에 청구하는 것으로 요양급여에 대한 구제적인 내역을 기재한 양식을 말한다. 명세서에는 요양기관에 관한 정보 및 환자의 요양급여 또는 비급여 내역, 인적 정보, 개인식별정보 등이 명시되어 있다. 건강보험심사평가원의 진료정보는 요양기관이

---

33) 건강보험심사평가원.
https://www.hira.or.kr/dummy.do?pgmid=HIRAA070001000310

34) 국민건강보험법 제42조(요양기관) ① 요양급여(간호와 이송은 제외한다)는 다음 각 호의 요양기관에서 실시한다. 이 경우 보건복지부장관은 공익이나 국가정책에 비추어 요양기관으로 적합하지 아니한 대통령령으로 정하는 의료기관 등은 요양기관에서 제외할 수 있다. <개정 2018. 3. 27.>.
1. 「의료법」에 따라 개설된 의료기관
2. 「약사법」에 따라 등록된 약국
3. 「약사법」 제91조에 따라 설립된 한국희귀·필수의약품센터
4. 「지역보건법」에 따른 보건소·보건의료원 및 보건지소
5. 「농어촌 등 보건의료를 위한 특별조치법」에 따라 설치된 보건진료소

35) 국민건강보험법 제41조(요양급여) ① 가입자와 피부양자의 질병, 부상, 출산 등에 대하여 다음 각 호의 요양급여를 실시한다.
1. 진찰·검사
2. 약제(藥劑)·치료재료의 지급
3. 처치·수술 및 그 밖의 치료
4. 예방·재활
5. 입원
6. 간호
7. 이송(移送)
② 제1항에 따른 요양급여(이하 “요양급여”라 한다)의 범위(이하 “요양급여대상”이라 한다)는 다음 각 호와 같다. <신설 2016. 2. 3.>
1. 제1항 각 호의 요양급여(제1항제2호의 약제는 제외한다): 제4항에 따라 보건복지부장관이 비급여대상으로 정한 것을 제외한 일체의 것
2. 제1항제2호의 약제: 제41조의3에 따라 요양급여대상으로 보건복지부장관이 결정하여 고시한 것.

36) 국민건강보험법 제44조(비용의 일부부담) ① 요양급여를 받는 자는 대통령령으로 정하는 바에 따라 비용의 일부(이하 “본인일부부담금”이라 한다)를 본인이 부담한다. 이 경우 선별급여에 대해서는 다른 요양급여에 비하여 본인일부부담금을 상향 조정할 수 있다. <개정 2016. 3. 22.>.

정보주체인 환자에게 실시한 요양급여가 적정하였는지 평가하고 그 비용을 심사하는 과정에서 필요한 정보를 말한다. 환자의 인적사항 등 정보가 포함되어 의료법 제23조의3 및 제23조의4의 취지와 범위가 같다고 할 수 없다.

진료정보는 의료인이 작성한 진료기록부 등의 기록만을 말하는 것으로 좁게 해석할 수 있으나 제23조의3 및 제23조의4의 진료정보는 전자의무기록에 저장·보관된 진료기록의 침해에 관한 규정으로 앞서 본 진료기록부 등에 기재한 기록 및 환자의 일반정보 모두를 포함한다고 해석될 수 있다.

라. 소결

의료법 제19조의 '정보', 제23조의 전자의무기록의 '개인정보', 제23조의3 및 제23조의4의 '진료정보' 등 법령 자체에서 사용되는 용어가 각각 다르고 적용 범위가 구체적으로 명시되어 있지 않았다. 그러나 그 용어가 사용된 법령의 전반적인 체계와 취지·목적 등을 종합적으로 고려[37]해 보건대 환자의 개인정보가 수집·작성·보관된 서식·형태만 다를 뿐 보호되는 개인정보에 있어 차이를 두지 않고 있었다.

진료 신청 과정에서 수집되는 성명, 주민등록번호, 연락처, 건강보험 등 '주관적 정보', 진료 과정에서 수집되는 진료 정보, 조산 정보, 간호 정보, 수술 정보 등 '객관적 정보'와 '가치판단정보', 처방 과정에서의 '처방의약품 정보', '진료비 정보' 등 모두 관리적, 기술적, 물리적 보호조치를 통하여 안전하게 보관되어야 하는 정보에 속한다.

3. 개인정보 침해 유형

가. 개인정보 보호 원칙

개인정보보호법은 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려

37) 대법원 2013. 12. 12. 선고 2011도9538 판결.

지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리"[38]인 개인정보자기결정권을 보장하고 있다.

개인정보자기결정권을 보장하기 위해서는 "개인정보의 수집, 이용, 제공 등 처리에 있어 정보주체의 동의 등 정당한 절차에 의해 이루어져야 하며, 내부자의 고의나 관리 부주의 또는 외부 공격으로 인해 유출·변조·훼손되지 않도록 안전하게 관리되어야 한다. 또한 개인정보를 보호하기 위하여 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 하며, 처리 목적 범위 안에서 정확성, 안전성, 최신성이 보장되고, 이 외 처리 목적의 명확화, 이용 제한, 안전 보호, 개인정보 처리 공개 원칙, 정보주체의 권리보장, 개인정보처리자의 책임 원칙 등"[39] 개인정보 보호 원칙을 준수하여야 한다.

개인정보 보호 원칙에 따라 의료기관은 환자의 개인정보를 최소한으로 수집하여야 하며, 최소한의 범위 내에서 이용하여야 한다. 개인정보보호법 제15조[40]에 따라 의료기관이 개인정보를 수집·이용하기 전에 ① 환자·보호자 등

---

38) 헌법재판소 2005. 5. 26. 99헌마513.

39) 개인정보보호법 제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.
② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.
③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.
④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.
⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적을 달성할 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다. <개정 2020. 2. 4.>
⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

40) 개인정보보호법 제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할

동의를 받아야 하는지 ② 의료법 등 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우인지 ③ 환자와의 계약 및 이행을 위하여 불가피하게 필요한 경우인지 ④ 환자 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 환자 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우인지 ⑤ 소송 제기 및 진행 등을 위하여 증빙자료를 조사하고 확보하는 경우 의료기관의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 환자의 권리보다 우선하는지 확인하여야 한다.

또한 환자의 개인정보를 수집·목적 외의 용도로 이용하거나 제3자에게 제공하기 위해서는 위의 ① 내지 ③의 내용을 확인하는 것이 필요하다.

수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 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 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다. <신설 2020. 2. 4.>

나. 금지되는 개인정보 침해 유형

의료법 제19조제1항은 의료인이나 의료기관 종사자가 관련 업무에 종사하면서 알게 된 다른 사람의 정보를 “누설 또는 발표”하지 못하게 하고 있으며, 제21조의2제8항 진료기록부전송지원시스템에 저장된 정보를 누구든지 정당한 사유 없이 “누출·변조 또는 훼손”하거나 제23조제3항의 전자의무기록에 저장된 개인정보를 정당한 사유 없이 “탐지, 누출·변조·훼손”을 금지하고 있다.

환자의 개인정보자기결정권을 침해하는 불법행위 유형은 매우 다양하며 이를 일률적으로 객관화하는 것은 어려우므로[41] 개인정보 처리 과정에서 발생하는 침해 유형으로 비교하여 살펴보면, ① 제19조제1항의 “누설 또는 발표”는 개인정보를 무단으로 다른 사람에게 제공하거나 공공연히 외부에 공개하거나 유출시키는 것으로 개인정보에 대한 접근 권한이 없는 자가 누설로 인하여 해당 개인정보에 접근할 수 있도록 하는 행위[42]를 말한다. 형법 제317조의 업무상비밀누설죄의 누설도 비밀에 속하는 사실을 아직 모르는 타인에게 알리는 것으로 구두·서면·작위·부작위 등 그 방법에는 제한이 없으며, 상대방은 1인이거나 다수이어도 상관없다[43]고 하여 의료법과 형법의 누설에 대한 해석은 유사하다고 할 수 있다. 개인정보 누설은 개인정보 처리 전체 과정인 수집·생성부터 파기에 걸쳐 발생할 수 있다.

② 제21조의2제8항 및 제23조제2항의 “정당한 사유 없이”란 처음부터 개인정보 처리에 관한 권한을 부여받지 못하였거나 부여받은 권한을 박탈당한 상태에서 마치 권한이 있는 것처럼 한 행위[44]를 말하며, ③ “유출”은 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우, 개인정보처리시스템에 권한이 없는 자가 접근한 경우, 고의 또는 과실로 인

41) 정부균, “환자 의료정보 보호의 문제”, 의료법학(제9권 2호), 대한의료법학회, 2008. 9, 365면.
42) 행정안전부, 위의 책, 359면.
43) 배종대, 위의 책, 230면.
44) 행정안전부, 위의 책, 359면.

하여 개인정보가 포함된 파일 또는 종이문서, 기타 저장매체가 권한 없는 자에게 잘못 전달된 경우, 그 밖에 권한 없는 자에게 개인정보가 전달되거나 개인정보처리시스템 등에 접근 가능하게 된 경우[45] 등 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고 환자의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용하는 행위를 말한다.

④ "훼손"은 타인의 개인정보를 조작, 일부를 지우거나 다르게 만들어서 본래의 개인정보의 특성, 효용 및 사회적 가치를 손상시키고 침해하는 행위[46]로 개인정보 처리 과정 중 파기 외 전체 과정에서 불법행위가 일어날 수 있으며, 개인정보를 삭제·폐기·소각 등을 하여 없애는 ⑤ "멸실"은 개인정보 처리 중 불법적인 파기를 말한다.

⑥ "변조" 행위에 대하여 대법원은 "환자를 진료한 당해 의료인은 의무기록 작성권자로서 보다 정확하고 상세한 기재를 위하여 사후에 자신이 작성한 의무기록을 가필·정정할 권한이 있다고 보이는 점, 2011. 4. 7. 법률 제10565호로 의료법을 개정하면서 허위작성 금지규정(제22조 제3항)을 신설함에 따라 의료인이 고의로 사실과 다르게 자신이 작성한 진료기록부 등을 추가기재·수정하는 행위가 금지되었는데, 이때의 진료기록부 등은 의무기록을 가리키는 것으로 봄이 타당한 점, 문서변조죄에 있어서 통상적인 변조의 개념 등을 종합하여 보면, 전자의무기록을 작성한 당해 의료인이 그 전자의무기록에 기재된 의료내용 중 일부를 추가·수정하였다 하더라도 그 의료인은 의료법 제23조 제3항에서 정한 변조행위의 주체가 될 수 없다고 보아야 한다."고 판시하였다. 형법 제231조의 변조는 "권한 없는 자가 이미 진정하게 성립된 타인 명의의 문서 내용에 대하여 동일성을 해하지 않을 정도로 변경을 가하여 새로운 증명력을 작출케 함으로써 공공적 신용을 해할 위험성이 있을 때 성립한다."[47] 이에 따라 의료인 본인이 작성한 자기명의의 전자의무기록에 추가기재·수정을 한 경우 변조 행

45) 보건복지부 및 행정안전부, 위의 책. 110-111면.
46) 행정안전부, 위의 책, 359면.
47) 대법원 2011. 9. 29. 선고 2010도14587 판결.

<표 1> 의료관련법령의 개인정보 유출 등 침해행위에 대한 벌칙

적용법조	주체	침해 객체	침해 행위	법정형
의료법 제87조의2제2항	제한 없음	진료기록전송 지원 시스템· 전자의무 기록의 개인정보	탐지, 누출, 변조, 훼손	5년 이하의 징역 또는 5천만원 이하의 벌금
의료법 제88조	의료인, 의료기관 종사자	업무상 알게 된 정보	비밀, 발표	3년 이하의 징역 또는 3천만원 이하의 벌금
지역보건법 제32조제1항 제1호	제한 없음	지역보건의료 정보 시스템의 정보	훼손, 멸실, 변경, 위조, 유출	5년 이하의 징역 또는 5천만원 이하의 벌금
지역보건법 제32조제1항 제2호	업무 종사자	업무상 알게 된 정보	사용, 제공, 누설	5년 이하의 징역 또는 5천만 원 이하 벌금
지역보건법 제32조제1항 제2호	영리 목적 부정한 목적	업무상 알게 된 정보	제공 받음	5년 이하의 징역 또는 5천만원 이하 벌금
지역보건법 제32조제3항	제한 없음	지역보건의료 정보 시스템의 정보	검색, 복제	3년 이하의 징역 또는 3천만원 이하 벌금
개인정보보호법 제70조제2호	거짓· 부정한 방법으로 개인정보 취득한 자	타인 처리 개인정보	제3자 제공, 교사· 알선	10년 이하의 징역 또는 1억원 이하의 벌금
개인정보보호법 제71조제5호	업무 종사자	업무상 알게 된 개인정보	누설, 제공, 제공받은 자	5년 이하의 징역 또는 5천만원 이하 벌금
개인정보보호법 제71조제6호	개인정보 처리자	업무상 알게 된 정보	누설, 제공	5년 이하의 징역 또는 5천만원 이하 벌금

위에 해당하지 않으나 고의로 사실과 다르게 추가기재·수정하는 경우 또는 정당한 사유 없이 탐지·누출·변조 또는 훼손하는 행위는 처벌 대상이 된다.

다. 개인정보 침해에 대한 벌칙

의료관련법령에서 정보 누설 및 전자정보시스템에 저장된 개인정보를 정당한 사유 없이 유출·변조·훼손 등 침해한 경우 이에 대한 벌칙 규정을 두고 있

다. 각 법령의 목적 및 취지, 관련 업무의 특수성 등을 고려하여 벌칙이 다르게 규정되어 있으나 대체로 중하게 벌하고 있다. 개인정보보호법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호하기 위해 제정·시행되었으나 카드사 개인정보 유출 사고[48]와 같은 대형 개인정보 유출이 빈발하여 개인정보 불법 유통으로 얻은 범죄 수익을 몰수·추징하고 부정한 방법으로 개인정보를 취득하여 영리 등 목적으로 타인에게 제공한 자에 대한 제재수준을 강화[49]하였다.

「지역보건법」은 일부개정을 통해 금융정보, 신용정보, 보험정보 및 그 외 개인정보에 대한 목적 외 사용 등의 벌칙[50] 수준을 개인정보보호법의 벌칙 수준인 5년 이상의 징역 또는 5천만원 이하의 벌금으로 통일하여 형사처벌의 공정성[51]과 법적 안정성을 기하였다.

개인정보보호법과 의료관련법령에서의 벌칙 규정 형식은 법정형의 정도에 따라 침해 객체와 침해 행위로 구성되어 있어 법령마다 이를 파악하기 매우 곤란하다.

의료관련법령에서 업무 또는 직무상 환자의 개인정보를 처리하고 있는데 사용되는 용어나 적용 범위가 불명확하다. 법령의 제정 목적·취지 및 규정 사

---

48) YTN, "카드사 사장들, 피해 최소화 노력할 것", 2014. 1. 20. https://www.ytn.co.kr/_ln/0102_201401201200477621

49) 법제처, 법률 제13423호, 2015. 7. 24. 일부개정

50) 지역보건법 제32조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2017. 9. 19.>
1. 제5조제3항을 위반하여 정당한 접근 권한 없이 또는 허용된 접근 권한을 넘어 지역보건의료정보시스템의 정보를 훼손·멸실·변경·위조 또는 유출한 자
2. 제28조를 위반하여 같은 조 제1호, 제2호 또는 제3호에 따른 정보를 사용·제공·누설한 자 및 그 사정을 알면서도 영리 목적 또는 부정한 목적으로 해당 정보를 제공받은 자
② 삭제 <2017. 9. 19.>
③ 제5조제3항을 위반하여 정당한 접근 권한 없이 또는 허용된 접근 권한을 넘어 지역보건의료정보시스템의 정보를 검색 또는 복제한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다. <개정 2017. 9. 19.>
1. 삭제 <2017. 9. 19.>
2. 삭제 <2017. 9. 19.>

51) 법제처, 법률 제14895호, 2017. 9. 19. 일부개정.

항은 각각 다르나 환자의 개인정보를 처리하는 것은 동일하므로 벌칙 규정을 달리 규정하고 있는 것은 정보주체와 정보처리자, 국민에게 혼란을 줄 수 있다. 일반법인 개인정보보호법을 기본으로 의료법 및 관계 법령에 차등을 두지 않고 적정하게 규제하는 것이 바람직하다.

의료법의 업무상 알게 된 정보 누설행위에 대한 벌칙을 지역보건법과 개인정보보호법에서의 벌칙과 동일하게 규정할 필요가 있으며 친고죄 규정의 폐지와 영리 목적 또는 부정한 목적으로 개인정보를 제공받은 자도 함께 처벌할 필요가 있다.

개인정보 처리 중 제공을 한 자와 제공을 받은 자를 필요적 공범 중 대향범으로 보아 동일하게 처벌하는 개인정보보호법에 따라 의료법도 영리 목적 등으로 개인정보를 제공받은 자를 처벌할 수 있게 규정하는 것이 특별법 우선 적용의 원칙을 고려할 때 적절하다.

IV. 마치며

개인정보는 유형자산과는 달리 소비되어 사라지지 않고 다른 사람이 동일한 정보를 계속 이용 및 복제를 통해 재생산할 수 있으며, 의료기관 뿐만 아니라 기업, 개인이 다발적으로 이용[52]할 수 있어 관리 · 보안을 철저히 하여야 한다.

의료기관에서 처리하는 환자의 개인정보에는 인적 정보 및 고유식별정보, 의료건강정보, 사회관계정보, 재산정보 등 여러 가지 민감정보 등이 있다. 이러한 환자의 개인정보를 처리하는 법률로서 의료법을 포함한 의료관련법령[53]이 있으나 관련 조항에서 사용되는 용어의 정의나 적용 범위가 명확히 규정되어 있지 않아 판례의 해석에 맡겨져 있다.

---

52) 개인정보보호위원회,『개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석』, 2017. 10. 13-14면.

53) 지역보건법, 국민건강보험법, 응급의료에관한법률, 후천성면역결핍증예방법 등 개인정보에 관한 규정을 두고 있다.

현재 개인정보보호법이 시행되고 있으나 의료의 특수성을 고려할 때 특별법인 의료법이 현실적으로 의료정보 등을 보호할 수 있도록 용어 등이 목적 및 취지에 맞게 정비되어야 할 것이며, 개인정보 침해행위에 대한 벌칙도 정보주체와 정보처리자, 국민의 형사처벌에 대한 공정과 법적 안정성을 기하여야 할 것이다.

환자의 개인정보 보호와 활용은 동전의 양면과 같으며, 의료기관에서 처리하는 개인정보는 민감정보로서 그 활용에 있어 더욱 신중하여야 할 것이다. 의료인 등 정보처리자는 개인정보 보호 원칙을 따르고, 정보주체의 권리인 사생활의 비밀과 자유, 인간의 존엄과 가치 및 행복추구권에 근거를 둔 인격권, 개인정보자기결정권을 보장[54]하여야 할 것이다.

54) 헌법재판소 2005. 5. 26. 99헌마513.

[참 고 문 헌]

김한나·이얼·김계현·이정찬·이평수, “개인의료정보의 관리 및 보호”, 『대한의사협회정책연구소 연구보고서』, 2013.

개인정보보호위원회, 『개인정보의 가치와 개인정보 침해에 따른 사회적 비용 분석』, 2017.

보건복지부 및 행정안전부, 『개인정보 보호 가이드라인 - 의료기관편』, 2015. 2.

배종대, 『형법각칙』 제10전정판, 홍문사, 2018.

의료정책연구소, 『의료정보의 보호와 관리방안』, 2012.

정부균, “환자 의료정보 보호의 문제”, 『의료법학』 제9권 2호, 대한의료법학회, 2008.

조홍석, “위험사회에 있어 개인의 의료정보 보호방안”, 『한양법학』 제24권 4집, 한양법학연구소, 2013.

행정안전부, 『개인정보 보호법령 및 지침·고시 해설』, 2011.

[국문초록]

의료법의 개인정보보호에 관한 연구

성수연(단국대학교 보건행정학과 강사)

의료기술의 발전과 환자 진료 향상 등을 목적으로 빅데이터나 인공지능에 의료정보를 분석·활용하면 유전적 질병이나 암 등 특이 질병 등에 대비할 수 있어 의료정보가 공유되어야 한다는 목소리가 높아지고 있다.

환자의 개인정보에 관한 활용과 보호는 동전의 양면과 같다. 의료기관 또는 의료인은 일반 정보처리자와 다른 환경적 특수성과 민감도가 높은 개인정보를 처리함에 있어 신중하여야 한다.

대체적으로 환자의 개인정보는 의료인이나 의료기관에서 수집・생성부터 파기까지 개인정보를 처리하고 있으나 의료법의 개인정보에 관한 용어 사용의 혼재되어 있거나 적용 범위가 명확하지 않아 판례의 해석에 의존하고 있다.

의료법 제23조의 전자의무기록에 저장・보관된 개인정보는 고유식별정보만을 의미하는 것이 아니라 진료기록부 등 의무기록의 개인정보와 동일하며, 그 내용은 인적 정보, 고유식별정보, 진료정보, 재산정보 등을 포함한다.

의료인이나 의료기관 개설자는 의료법 제24조의4 진료정보가 침해된 경우 제23조의 개인정보와 동일하게 취급하여야 하는지에 대해 전자의무기록에 환자의 민감정보가 기록·저장·보관되어 있으므로 특별히 개인정보 중 진료정보만을 의미한다고 볼 수 없다.

의료법 제19조의 정보 누설 금지는 업무상 알게 된 '비밀'에서 '정보'로 개정되었으나 명칭만 바뀌었을 뿐 보호법익은 형법상의 비밀과 동일하여 환자의 개인정보자기결정권을 보호하고 있지 못하다. 개인정보보호법과 지역보건법은 '업무상 알게 된 정보'에서의 보호법익을 개인정보자기결정권으로 보아 누출, 위조, 변조, 훼손 등 개인정보 침해 행위에 대하여 동일하게 벌칙을 규정하고 있다.

의료법의 개인정보 보호 규정은 용어의 정의가 불명확하여 정보주체 및 정보처리자, 국민에게 적용 범위 등 혼란을 일으킬 수 있어 용어가 통일적으로 정비되어야 할 필요가 있으며, 개인정보 보호에 관한 특별법인 의료법과 일반법인 개인정보보호법의 규정 내용이나 범위가 일치하지 않아 해석상 혼란이 생길 수 있어 개인정보 보호에 대하여 일정한 한계를 보인다.

환자의 개인정보는 민감정보로서 그 활용과 처리에 있어 안전하게 보호되어야 한다.

개인정보 보호 원칙에 따라 개인정보를 처리하여야 하며, 정보주체인 환자나 보호자의 권리인 사생활의 비밀과 자유, 인격권, 개인정보자기결정권을 보장하여야 할 것이다.

주제어 : 개인정보, 진료정보, 개인정보자기결정권, 개인정보 침해, 의료법

A Study on the Protection of Personal Information in the Medical Service Act

Sung, Soo-Yeon

Lecturer, Department of Health Administration at Dankook University

=ABSTRACT=

There is a growing voice that medical information should be shared because it can prepare for genetic diseases or cancer by analyzing and utilizing medical information in big data or artificial intelligence to develop medical technology and improve patient care.

The utilization and protection of patients' personal information are the same as two sides of the same coin. Medical institutions or medical personnel should take extra caution in handling personal information with high environmental distinct characteristics and sensitivity, which is different from general information processors.

In general, the patient's personal information is processed by medical personnel or medical institutions through the processes of collection, creation, and destruction. Still, the use of terms related to personal information in the Medical Service Act is jumbled, or the scope of application is unclear, so it relies on the interpretation of precedents.

For the medical personnel or the founder of the medical institution, in the case of infringement of Article 24(4), it cannot be regarded that it means only medical treatment information among personal information, whether or not it should be treated the same as the personal information under Article 23, because the sensitive information of patients is recorded, saved, and stored in electronic medical records.

Although the prohibition of information leakage under Article 19 of the Medical Service Act has a revision; 'secret' that was learned in business was

revised to ‘information’, but only the name was changed, and the benefit and protection of the law is the same as the ‘secret’ of the criminal law, such that the patient’s right to self-determination of personal information is not protected.

The Privacy Law and the Local Health Act consider the benefit and protection of the law in ‘information learned in business’ as the right to self-determination of personal information and stipulate the same penalties for personal information infringement such as leakage, forgery, alteration, and damage.

The privacy regulations of the Medical Service Act require that the terms be adjusted uniformly because the jumbled use of terms can confuse information subjects, information processors, and shows certain limitations on the protection of personal information because the contents or scope of the regulations of the Medical Service Law for special corporations and the Privacy Law may cause confusion in interpretation.

The patient’s personal information is sensitive and must be safely protected in its use and processing. Personal information must be processed in accordance with the protection principle of Privacy Law, and the rights such as privacy, freedom, personal rights, and the right to self-determination of personal information of patients or guardians, the information subject, must be guaranteed.

Keyword : Personal information, medical information, right to self-determination of personal information, infringement of personal information, Medical Service Act