成均館大學校 比較法硏究所
成均館法學 第17卷 第2號 2005年 12月
SungKyunKwan Law Review
The Institute for Comparative Legal Studies
Vol. 17 No. 2 December. 2005

의료정보의 현황과 입법과제

김 민 호*

Ⅰ. 연구의 배경 및 목적

지식정보화산업사회에서 의료분야 역시 다른 분야와 마찬가지로 정보통신기술을 활용하는 정보시스템의 구축, 표준화, 공동이용 등의 문제에 대하여 무관심할 수는 없을 것이다. 이미 의료계에서는 정보통신기술의 발달에 따라 의료의 인프라 변화, 진료의 대중화, 진료·처방의 통합화 등이 가속화될 것으로 예상하고 의료정보시스템의 구축에 적극적 투자를 하고 있다. 초기의 의료정보시스템은 의료기관의 단순 사무처리 시스템의 구축에서 출발하였으나 현재에는 환자의 병력관리, 임상연구자료관리 등으로 그 범위를 더욱 확대해 가고 있으며 궁극적으로 의료정보의 기관 간 공동

* 성균관대학교 법과대학 교수, 법학박사.

활용시스템의 구축을 모색하고 있다.

이러한 의료환경의 급속한 변화에 발맞추어 법제의 연구 및 입법활동 등도 병행적으로 이루어져야함에도 불구하고 지금의 현실은 그러하지 못한 실정이다. 시기적으로 매우 늦은 감은 있으나 지금이라도 보다 적극적으로 관련 법제에 대한 연구와 입법활동 등이 전게되어야 할 것이다. 물론 '의료정보'를 '개인정보'라는 커다란 틀 속의 일부분으로 이해한다면, 이미 개인정보와 관련한 시스템의 개발, 구축, 활용, 공동이용, 보호 등의 법제들이 존재하고 있는 까닭에 법제의 진공은 초래하지 않을 것이라고 안도할 수도 있을 것이다. 그러나 우리는 이미 교육정보시스템의 구축 등과 관련하여 커다란 홍역을 경험한 바 있다. 사건의 발단은 교육정보를 개인정보의 한 단면에 불과한 것으로 단순 이해함으로써 발생되었다고 해도 과언이 아닐 것이다. 마찬가지로 의료정보 역시 개인정보의 한 단면으로 취급하면서 문제를 접근해 간다면 커다란 혼란과 치유할 수 없는 문제를 발생시킬 수 있을 것이다. 따라서 '의료정보'의 정확한 개념과 특질을 이해하는 작업이 무엇보다 선행되어야 할 것이다.

Ⅱ. 의료정보와 의료정보시스템

1. 의료정보의 의의

의료정보란 '의료제공의 필요성을 판단하기 위하여 또는 의료제공을 행하기 위하여 진료 등을 통해서 얻은 환자의 건강상태 등에 관한 정보'라고 정의하면서, 이를 다시 ①환자의 기본정보, ②건강보험과 복지정보, ③진료관리용정보, ④생활배경정보, ⑤의학적 배경정보, ⑥진료기록정보, ⑦지시실시기록정보, ⑧진료정보교환정보, ⑨진료설명과 동의정보, ⑩요약정보, ⑪사망기록정보 등으로 세분화 하여 설명하는 견해도 있고,[1] '개인의 과거·현재·미래의 육체적·정신적 건강, 의료서비스를 받았던 사실 및 의료서비스에 대한 대가를 지급사실 그리고 인구통계학적 사실 등을 담고 있는 정보'라고 하면서 이러한 의료정보를 구성하는 요소에는 성명, 주소, 나이, 양친의 이름, 출생지, 출생연원일, 결혼상황, 종교, 병역사항, 주민등록번호, 가입보험회사명, 병력, 주요증상, 진단결과, 사회력, 가족력, 과거의 치료방법, 신체각부위의 상황, 약물요법, 음주량, 흡연량 등이 있다고 설명하는 견해[2]도 있다.

1) 백윤철, 우리나라에서 의료정보와 개인정보 보호, 헌법학연구 제11권 제1호, 418면, 한국헌법학회, 2005.3.

한편, 「보건의료기본법」[3] 제3조 6호는 '보건의료정보'를 '보건의료와 관련한 지식 또는 부호·수자·문자·음성·음향 및 영상 등으로 표현된 모든 종류의 자료'라고 정의하고 있다.

2. 의료정보시스템의 의의

의료정보시스템이란 의료정보를 전자적으로 저장하고 활용하기 위해 구축된 시스템을 말한다. 의료정보시스템은 정보의 활용목적에 따라 ①업무처리시스템(TPS : Transection Processing System), ②정보보고시스템(IRS : Information Reporting System), ③의사결정지원시스템(DSS : Decision Support System), ④사무자동화시스템(OS : Office Automation)으로 크게 구분된다. 특히 업무처리시스템은 대상 업무의 성격에 따라 ①원무관리시스템, ②진료업무시스템, ③진료지원시스템, ④관리지원시스템으로 나눌 수 있다. 최근 대형 의료기관들이 구축 또는 구축 중에 있는 처방전달시스템(OCS : Order Communication System), 영상정보관리시스템(PACS : Picture Archiving Communication System), 전자의무기록시스템(EMR : Electronic Medical Record) 등은 진료업무 또는 진료지원업무시스템의 일종이다.[4]

한편, 의료정보시스템은 '제1단계 : 단순 사무처리 단계, 제2단계 : 진료업무 지원단계, 제3단계 : 병원기능 향상 단계, 제4단계 : 병원 경영기능 향상 단계, 제5단계 : 병원의 전략적 의사결정 지원 단계' 등과 같이 단계적으로 발전·진화 되고 있다.[5]

Ⅲ. 의료정보화의 현황

「보건의료기술진흥법」[6] 제8조는 '보건복지부장관은 보건의료정보의 생산·유통 및 활용을 위하여 1. 보건의료정보의 관리를 위한 전문연구기관의 육성, 2. 보건의료·복지분야의 전산화 촉진을 위한 업무의 표준에 관한 연구·개발 및 관리, 3. 보건의료

2) 김형기, 보험회사간 의료정보 공유제도, 보험학회지 제65집, 79면, 한국보험학회, 2003.8.
3) 일부개정 2003.5.29 법률 6909호.
4) 이귀원, 원격의료정보 시스템의 활성화 방안에 관한 연구, 대한방사선기술학회지 Vol.26, No.4, 54면, 2003.
5) 이귀원, 앞의 글, 54면.
6) 일부개정 2003.5.29 법률 6909호.

정보의 공동이용 활성화, 4. 기타 보건복지부령이 정하는 보건의료정보의 진흥에 관한 중요사업 사업 등을 추진한다.'라고 규정하고 있다.

보건복지부는 의료기관간의 진료정보공유를 위한 '전자건강기록(EHR)' 사업을 추진중에 있으며, 2005년 초, 분당서울대병원, 연세의료원, 동산의료원을 EHR 핵심기반기술개발센터로 지정, 향후 6년간 ①국제표준에 부합한 전자건강기록 시범 구축, ②환자 정보공유 시스템 개발, ③진료정보 공유 네트워크 등을 개발할 계획이다.

2005년 4월, 서울특별시 노원구는 tele-PACS(원격영상정보관리시스템)의 개발사업에 착수하여 조만간 본격운영에 들어갈 예정이다. 이 시스템은 환자의 방사선 검진결과를 디지털 영상으로 담아 메인컴퓨터에 저장·활용하는 장치로 재생 및 전송이 가능하도록 구축되는 것으로서, 지역 주민들이 보건소에서 흉부 X-선 검진을 받고, 관내 종합병원 진단방사선과 전문의의 원격판독을 통해 호흡기질환에 대한 정확한 진단을 받을 수 있도록 설계된 것이다. 진단방사선 전문의가 없는 의료취약지구 주민들의 의료서비스 향상을 위해 크게 기여할 것으로 평가되고 있다.

이미 대형 의료기관들은 정보화의 수준과 단계적인 차이는 있지만 자체적으로 의료정보시스템을 구축·운용하고 있으며, 정부차원에서도 EMR, PACS 등의 시스템 개발·구축에 적극적 태도를 보이고 있다.

Ⅳ. 의료정보화에 대한 미국의 법제 동향

1. 의료정보에 관한 법률

선행연구 문헌들에서 언급하고 있는 미국 MIB(Medical Information Bureau)의 NAIC(National Association of Insurance Commissioners)프라이버시보호표준모델법(1978)이나, Uniform Health Care Information Act 등은 미국법령정보시스템에서 확인할 수 없었다. 다만, 미국 현행법상 의료정보와 관련한 것으로는 Health Insurance Portability and Accountability Act(1996, 이하 'HIPAA'라 함)[7]가 있다. 주지하는 바처럼, 미국의 법령체계는 우리나라와 달리 독립된 단일 법률이 존재하는 것이 아니라, 특정법령의 규정들이 미국연방법령집(United States Codes)의 여기저기에 산재되어 있다. HIPAA 역시 US Codes title 29, 42, 18, 26 등에 분산 규정되어 있는 57개 조문을 묶어서 지칭하는 일종의 별칭(popular code name)이다. 이러한 HIPAA 중에서 US

7) Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936.

Code title 42의 §1320d부터 §1320d-8까지 9개 조문[8]이 의료정보에 관한 내용을 규정하고 있다.

§1320d는 의료정보(health information)에 대해 '(A)의료제공자, 의료보험자(health plan)[9], 공공의료행정기관, 고용자, 생명보험회사, 학교, 대학, 기타 의료정보처리자[10](health care clearinghouse)[11]에 의해 생성 또는 수집된 것과, (B)개인의 과거, 현재, 미래의 육체적·정신적 건강상태, 진료제공, 진료제공에 대가의 지급 등의 42 C.F.R. § 1001.952(k)(2)사실[12]에 대한 모든 문언 또는 기록적 정보를 말 한다'라고 규정하고 있다.

§1320d-2는 정보이용과 데이터 구성요소의 기준에 대해 규정하고 있다. (a)항은 동법의 시행이후 12개월 이내에 보건복지부장관(the Secretary of Health and Human Services)으로 하여금 의료정보의 privacy보호에 관한 자세한 준칙(standards, 일종의 법규명령)을 정하여 상하 양원의 노동·인적자원위원회, 재정위원회 등에 제출할 것을 규정하고 있다. (b)항은 보건복지부장관이 privacy보호준칙을 마련할 때에 (1)개인 식별이 가능한 의료정보의 주체가 향유할 수 있는 권리의 구체적 내용, (2)당해 권리의 행사를 위한 절차, (3)정보의 사용 및 폐기에 대한 요구권 등의 사항을 반드시 포함하도록 권고 하고 있다. (c)(1)항은 당해 준칙의 제정 시한에 대해 규정하고 있고, (2)항은 당해 준칙이 개인 식별 의료정보에 대해 보다 엄격하게 규정하고 있는 주법률에 우선할 수 없음을 규정하고 있다.

§1320d-4는 §1320d에서 규정하고 있는 의료정보를 처리하고자 하는 자에 대해 보건복지부장관이 제정하는 준칙의 준수의무를 규정하고 있다. (a)(1)항은 일반규정으로서 (A)의료정보처리준칙에 반하는 정보처리를 수행할 수 없으며, (B)보험회사 역시 의료정보준칙에 반하는 정보처리를 할 수 없으며, (C)의료정보처리를 위한 수집정보 또는 취급정보는 반드시 준칙에서 정하는 데이터 구성요소에 합치되어야 함을 규정

8) 42 USCA §1320d, §1320d-1, §1320d-2, §1320d-3, §1320d-4, §1320d-5, §1320d-6, §1320d-7, §1320d-8.

9) health plan이란 의료서비스제공자와 의료제공계약을 체결하여 의료제공자로 하여금 보험료 또는 수수료를 납부한 회원들에게 의료서비스를 제공하도록 하는 자(단체)를 말한다. 42 C.F.R. § 1001.952(k)(2)

10) health care clearinghouse이란 영수증 발급, 의료보험자 정보, 의료기관정보, 보험계약자의 의료정보 등을 처리하는 사적, 공적 조직을 말한다.45 C.F.R. § 160.103 (2).

11) 42 USCA §1320d(A).

12) 42 USCA §1320d(B).

하고 있다. (a)(2) 및 (3)항은 의료정보처리자들이 정보처리절차 및 내용을 정보처리준칙에서 규정하고 있는 기준에 합치시켜야 하는 시한을 규정하고 있고, (b)항 역시 소규모 의료기관에 대한 준칙적응시한에 대해 규정하고 있다.

§1320d-5는 준칙에 반하는 행위에 대한 벌칙을 규정하고 있는 바, 행위위반에 대해 벌금은 1회에 $100, 연간통산 $25,000를 넘지 못한다고 규정하고 있다. (a)(2)항 이하에서는 과벌절차 등에 대해 규정하고 있다.

§1320d-6은 개인 식별 의료정보의 불법적 공개에 대해 규정하고 있는 바, (a)항은 불법 공개의 범죄유형으로서 (1)특수질병자의 신원공개, (2)개인 식별 의료정보의 불법적 수집, (3)개인 식별 정보의 제3자에 대한 유출 등을 규정하고, (b)항에서는 단순한 수집 등의 경우에는 $50,000 이하의 벌금과 1년 이하의 징역, 사기 기타 불법적 수단을 사용한 수집 등에는 $100,000 이하의 벌금과 5년 이하의 징역, 수집된 정보의 판매 등에는 $250,000 이하의 벌금과 10년 이하의 징역에 처할 수 있음을 규정하고 있다.

§1320d-7은 동법과 주법률의 관계에 대한 규정으로서, 주법률은 동법의 내용에 반하여 제정될 수 없으나, 동법보다 더욱 엄격히 규정된 주법률은 동법보다 우선 적용한다는 내용을 담고 있다.

HIPAA에 근거한 the Secretary of Health and Human Services의 standards는 "Code of Federal Regulations, Title 45, Part 164"에 36개의 조문으로 규정되어 있다.[13]

2. 의료정보에 관한 대통령집행명령

HIPAA의 시행을 위하여 대통령의 집행명령(Executive Order)[14] 13181호가 2000년 12월에 제정되었다. 그 내용을 요약하면 다음과 같다.

Section 1. Policy : 의료정보는 공공의 이익과 의사-환자간의 치료, 또는 환자를 위한 의료서비스의 제공을 위한 경우가 아니면 어떠한 경우에도 사용되어져서는 안 된다.

개인 식별 의료정보(보호되는 의료정보)에 대한 privacy보호를 위하여 HIPAA에 근

13) CODE OF FEDERAL REGULATIONS, TITLE 45--PUBLIC WELFARE, SUBTITLE A--DEPARTMENT OF HEALTH AND HUMAN SERVICES, SUBCHAPTER C--ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS, PART 164--SECURITY AND PRIVACY.

14) EXECUTIVE ORDER NO. 13181, Dec. 20, 2000, 65 F.R. 81321.

거한 보건복지부장관의 준칙을 마련하고 있다. 그런데 HIPAA는 의료제공자, 의료정보처리자 등과 같이 법에 의해 '특정된 자(covered entities)'에게만 적용이 되는 까닭에 법에서 정하고 있지 아니한 단체나 개인에게는 적용이 되지 아니한다. 예를 들면 보건을 담당하고 있는 연방 행정공무원이 직무수행과정에서 얻게 된 의료정보에 대해서는 이 법이 적용되지 않는 것으로 해석될 수 있다. 따라서 새로이 제정될 HIPAA 시행령(보건복지부장관의 준칙)은 이러한 경우에 대비하는 규정을 마련하여야 할 것이다. 특히 보건감독관들이 조사활동을 함에 있어서는 보건진료가 법을 위반하지는 않았는가? 또는 진료과정상 사기행위는 없었는가? 등을 조사하기 위하여 개인 식별이 되지 아니하는 불특정 다수의 의료기록을 조사할 수는 있으나 특정 개인의 의료정보를 조사할 수는 없다.

때로는 의료과정상의 사기 등과 같은 범죄행위를 수사 또는 형사소추하기 위해서 수사자가 보호되는 특정인의 의료정보를 액세스하는 것이 불가피한 경우도 발생하는 바, 이때에도 HIPAA시행령에 의한 엄격해석원칙이 그대로 적용되어져야 한다. 마찬가지로 행정목적의 수행을 위하여 의료정보에 대한 자료제출요구가 필요한 때에도 HIPAA시행령이 엄격히 적용되어져야 한다. 의료정보에 대한 증거채택 또는 자료제출요구 등의 판단은 판사의 권한이며, 판사는 이러한 결정을 함에 있어서 '당해 의료정보의 제공이 공공의 이익, 또는 의사-환자간의 치료, 환자를 위한 의료서비스의 제공을 위하여 반드시 필요한 것인가?'를 고려하여야 한다.

보건업무와 직접 관련이 없는 어떠한 민사적, 형사적, 행정적 조사활동도 앞에서 정립한 원칙-의료정보는 공공의 이익과 의사-환자간의 치료, 또는 환자를 위한 의료서비스의 제공을 위한 경우가 아니면 어떠한 경우에도 사용되어져서는 안 된다-을 위반하여서는 안 된다는 것을 다시 한 번 천명한다.

Sec. 2. Definitions. : '보건감독행위', '보호되는 의료정보'의 구체적 범위는 HIPAA 시행령으로 정한다. HIPAA의 문언상 'Injury to the patient'는 환자의 사익에 대한 침해도 포함한다.

Sec. 3. Implementation. : 보건업무와 직접 관련이 없는 어떠한 민사적, 형사적, 행정적 조사활동을 함에 있어서 '보호되는 의료정보'는 법무부 차관 또는 군인의 경우에는 국방부 법무감의 승인이 있는 때에만 사용할 수 있다. 법무부 차관은 당해 의료정보의 사용에 대한 승인여부를 판단함에 있어서 앞에서 정립한 원칙-의료정보는 공

공의 이익과 의사-환자간의 치료, 또는 환자를 위한 의료서비스의 제공을 위한 경우가 아니면 어떠한 경우에도 사용되어져서는 안 된다.-을 고려하여야 한다. 법무부 차관이 당해 '보호되는 의료정보'의 사용을 승인할 때에는 승인되지 아니한 사용을 방지할 수 있는 적절한 안전조치를 마련하여야 한다.

매년 법무부 장관은 보건복지부장관과 협의하여 아래의 사항에 대한 보고서를 대통령에게 제출하여야 한다.

(i) 보건업무와 직접 관련이 없는 조사활동에 '보호되는 의료정보'의 사용승인 요청건수

(ii) 사용승인 요청에 대한 승인율, 기각율, 수정율 등

(iii) 사용승인을 요청한 행정청 및 당해 행정청의 요청건수

(iv) '보호되는 의료정보'의 총 사용량

Sec. 4. Exceptions. : 이 집행명령은 보건업무와 관련이 없는 조사활동을 통하여 법집행공무원이 수집한 '보호되는 의료정보'의 파생적(제2차적, 가공적) 사용을 제한할 수는 없다. 또한 이 집행명령은 다른 법률에 의해 부과된 의무를 제한할 수 있는 것으로 해석되지 아니한다.

3. HIPAA 관련 판례

South Carolina Medical Association v. Thompson[15]사건은 HIPAA가 적용되는 의료정보에는 '전자적으로 처리된 의료정보' 뿐만 아니라 모든 의료정보가 모두 포함된다고 판시한 판례이다.

South Carolina의 의사협회는 HIPAA의 적용이 '전자의료정보' 뿐만 아니라 모든 의료정보에 적용되는 것은 위헌이므로 무효라는 '무효선언청구소송'을 제기하였다. 이에 보건복지부는 의료정보에 대한 개인의 privacy보호를 위해서는 전자의료정보와 종이의료정보를 분리할 수 없을 뿐만 아니라 전자정보와 종이정보를 실제로 분리하는 것도 불가능하다고 반론을 제기하였다.

이에 대해 법원은 "42 U.S.C.A. §1320d(4)에서 의료정보란 'any information, whether oral or recorded in any form or medium'이라고 규정하고 있는 바, 이는 보건복지부가 전자의료정보 뿐만 아니라 종이의료정보에 대해서도 준칙을 규정할 수 있는 것으로

15) 327 F.3d 346 (4th Cir. 2003), cert. denied, 124 S. Ct. 464 (U.S. 2003).

해석하는 것이 타당하다. 만약 HIPAA가 전자의료정보에만 적용된다면 의사들은 가능한 HIPAA의 적용을 받지 않는 종이의료정보를 선택할 것이며, 종이의료정보의 전산화도 기피할 것이다. 따라서 HIPAA가 의욕하는 소기의 목적을 달성하고 의료정보의 전산화를 촉진하기 위해서는 HIPAA의 적용범위가 전자정보뿐만 아니라 종이정보에까지 미치는 것으로 해석하는 것이 타당하다."라고 판시하였다.

한편, Association of American Physicians & Surgeons, Inc. v. U.S. Dept. Of Health and Human Services[16]사건은 HIPAA와 Privacy Rule과의 관계에 대한 판결이다. 미국내·외과의사협회는 'HIPAA의 적용범위가 전자의료정보 뿐만 아니라 종이의료정보에도 미치는 것은 위헌이다. 왜냐하면 이미 종이의료정보를 포함하는 일체의 개인정보에 대하여 규율하고 있는 Privacy Rule이 존재하기 때문에 HIPAA는 전자의료정보의 전달에 대해서만 적용되는 것으로 해석하는 것이 타당하다.'라고 주장하면서 HIPAA의 무효선언청구소송을 제기하였다.

이에 대해 법원은 'Privacy Rule은 의료정보뿐만 아니라 종이를 비롯한 어떠한 저장매체를 통하여 저장된 모든 개인정보에 대해 privacy보호를 규정하고 있고, HIPAA는 특히 의료정보에 대한 privacy보호를 규정하고 있는 바, 양법이 그 목적과 취지가 다르지 아니하므로 HIPAA에 근거한 준칙이 Privacy Rule의 규정에 직접적으로 반하지 않는 한 위헌이 아니다. 뿐만 아니라 HIPAA는 의료정보의 전산화를 촉진하고자 제정된 것이므로 이 법이 전자의료정보에만 적용된다고 하면 의료정보의 전산화를 기피할 우려가 있다. 따라서 HIPAA가 전자의료정보 뿐만 아니라 종이의료정보에 대해서도 적용된다고 규정한 것은 위헌이 아니다.'라고 판시하였다.

Ⅴ. 의료정보시스템 활성화를 위한 법제 정비 과제

의료정보시스템에 대한 사회적 인식은 정보화에 따른 역기능보다는 순기능에 대하여 많은 기대감을 가지고 있음을 부정할 수 없다. 의료정보시스템의 활성화 자체를 적극적으로 반대하는 사람은 없을 것이다. 그런데 문제는 앞에서 언급한 바와 같이 의료정보는 다른 개인정보들 보다도 개인의 privacy에 매우 치명적인 영향을 미칠 수 있는 이른바 '민감정보'를 많이 담고 있다는 것이다. 정보화의 효율성으로 발생가능한

16) 224 F. Supp. 2d 1115, 194 A.L.R. Fed. 711 (S.D. Tex. 2002), aff'd without opinion, 67 Fed. Appx. 253 (5th Cir. 2003).

치명적 개인정보의 침해에 대한 논의를 덮을 수는 없는 것이다. 그렇다고 의료정보시스템의 활성화라는 대세를 역행하자는 것은 결코 아니다. 의료정보시스템을 구축하고 이를 공동이용하기에 앞서 예상가능한 문제점을 검토해 보고, 이에 대한 해결방안을 모색하여 시스템의 구축과 이용에 대한 가이드라인을 조속히 마련하자는 것이다.

더욱 시급한 것은 의료정보시스템의 통합논의에 대한 검증이다. 왜냐하면 자칫 '의료정보의 공동이용'을 '의료정보데이터의 통합관리'로 오해할 가능성이 있으며, 실지로 법학 이외의 학문분야에서는 이미 의료정보데이터의 통합관리 시스템의 구축 및 그 유용성에 대하여 많은 논의들을 하고 있는 실정이다. 그러나 정보의 공동이용이라는 것이 항상 정보데이터의 통합관리를 의미하는 것은 아니다. 정보데이터의 통합관리는 정보공동이용을 위한 방법론 중의 하나에 불과하다. 다시 말해서 생성된 정보를 공동이용 한다는 것과 통합된 정보의 관리 주체가 모든 정보데이터에 자유롭게 액세스 할 수 있다는 것은 매우 다른 것이다.

의료정보시스템 활성화의 실익은 ①의료기간의 시스템구축 비용절감 및 경영합리화, ②의료기관과 보험회사 등의 정보공유를 통한 비용절감, ③환자의 의료서비스 향상 등일 것이다. 실지로 대형 의료기관들이 자체적인 의료정보시스템을 구축하면서 많은 예산을 투입하였고 이러한 투입예산은 결국 소비자에게 전가될 것이며 의료기관 자체의 경영부담으로 작용할 수 있다. 따라서 국가적 차원에서 또는 지역 연합적 단계에서 의료정보시스템을 통합적으로 구축한다면 이러한 시스템 구축비용을 절감할 수 있을 뿐만 아니라, 모든 의료기관이 고가의 첨단 의료장비를 모두 갖추고 있지 아니하여도 이를 공동으로 활용할 수도 있고, 특히 의료서비스취약지역에 대한 의료서비스의 질을 한층 높일 수도 있을 것이다. 그러나 의료정보의 전산화 내지는 시스템화가 반드시 통합형으로 구축되어야만 우리가 지금 기대하고 있는 이러한 실익들이 담보되는 것은 아니다.

의료정보통합시스템이 구축되어 있는 상태에서 어느 한 개인이 의료서비스를 받는 과정을 상정해보자. 1차 의료기관인 동내 의원에서 일단 진료를 받으면 성명, 주민등록번호, 주소, 전화번호 등의 개인 인적정보와 의사의 진료기록정보가 의원의 해당 서버에 저장이 될 것이고, 이 정보는 PKI인증을 거쳐서 Router를 통하여 통합서버로 전송될 것이다. 이때에 의사가 2,3차 의료기관으로의 진료의뢰서를 첨부할 것이다. 환자는 2,3차 의료기관에 내방하여 진료접수를 하면 당해 의료기관 역시 PKI인증을 거쳐 통합서버로 액세스한 다음 환자의 인적정보와 진료기록을 당해 병원의 서버로 올려서 이후 이루어지는 여러 가지 검사결과를 추가하여 기록한 다음 통합서버로 전송

하여 저장할 것이다. 환자를 면담하는 의사는 PKI인증을 통하여 통합서버에 저장되어 있는 환자의 의료정보를 자신의 데스크 컴퓨터에 올릴 것이다. 이후 또 여러 가지의 진료 및 처방기록이 추가될 것이며 이 또한 마찬가지의 과정을 거쳐 통합서버에 저장될 것이다. 만약 환자가 2,3차 의료기관을 또 옮기더라도 마찬가지의 프로세스를 거쳐 해당 의료정보가 담당의사의 데스크 컴퓨터에 뿌려질 것이다. 병원에서는 환자의 보험관련 정보를 추가하여 통합서버에 전송해 두면 보험관리공단은 환자의 보험관련기록을 통합서버에서 취득하여 보험료지급 등의 사무를 처리할 것이다, 더 나아가 환자가 사설 보험화사에 가입을 할 경우 보험회사는 통합서버에 액세스를 해서 보험가입자의 병력을 조회할 수도 있을 것이다. 이러한 시스템이 구축되면 1차 의료기관과 2,3차 의료기관의 유기적 협조체제 구축과 환자가 병원을 옮기는 경우에도 불필요한 중복 검사를 피할 수 있고, 특수한 고가 장비가 있는 병원에서 검사만을 하고 진단은 다른 병원에서 받을 수도 있는 등 그 효율성은 충분히 미루어 짐작이 간다. 그런데 문제는 한 개인의 기본인적정보와 의료정보가 결합된 '민감정보'가 어디서나 또한 누구에 의해서 너무나 쉽게 노출될 수 있다는 것이다. 물론 인증제도를 통한 액세스 권한의 엄격한 제한, 해킹 등의 방지를 통한 정보의 유출방지 등과 같은 장치를 당연히 마련하겠지만, 그러한 시스템적 또는 제도적 장치에도 불구하고 정보가 유출되었을 경우 개인이 당해야 하는 침해는 도저히 회복이 불가능할 수도 있다는 것이다. 정보수집에 대한 동의, 자기정보열람, 자기정보의 오류에 대한 정정청구, 자기정보이용금지, 정보의 목적 외 사용금지 등과 같은 개인정보보호를 위한 일반적 장치만으로는 완전한 보호를 기대하기가 어렵다는 것이다.

의료서비스는 효율성의 문제가 아니다. 진료 의사가 그 자리에서 약을 바로 조제해 주거나 반대로 약사가 문진 등을 통하여 발견한 질병에 대한 약을 직접 조제해 주는 것이 바로 효율이다. 그러나 우리는 의사의 처방과 약사의 조제를 분리해 두고 있다. 이는 의료가 효율성만을 추구해서는 안 되는 것을 직접적으로 반증하는 것이다. 의료는 효율성보다는 안전성이 더욱 중요한 과제인 것이다. 의료정보 역시 마찬가지이다. 효율성은 안전성의 범위 내에서 추구되어 져야 한다.

이미 대형 종합병원들은 자체 의료정보시스템을 구축·운용하고 있다. 서울대학교 병원에서 진료를 받는 다고 가정해 보자. 서울대학병원 어느 부서, 심지어는 원무과나 접수창구에서 조차도 환자의 성명, 주민등록번호, 주소 등의 인적정보와 진료정보의 액세스가 가능하다. MRI검사를 받는 환자가 김아무개이며 간이 아프며 담당의사가 이아무개라는 것을 병원 내에서는 인증키를 가진 사람은 누구나 쉽게 알 수 있다

는 것이다.

따라서 우리는 지금 의료정보시스템의 통합적 구축 문제를 논의하기에 앞서서 이미 구축되어 있는 또는 앞으로 구축될 개별 의료기관의 의료정보시스템에 대한 가이드라인부터 빨리 마련하여야 할 것이다. 아울러 의료정보시스템의 통합구축 보다는 표준화를 통한 필요정보 전송방식으로 시스템 개발의 방향을 전환하는 방안을 검토해 볼 필요가 있다.

Ⅵ. 바람직한 법제 정비 방향

1. 의료정보보호 법령의 입법방식

개인정보보호 법령의 입법방식에는 ①공적부문과 민간부분을 하나의 법률에 포괄하여 규제하는 통합방식, ②공적부문과 민간부문을 분리하여 각 각의 법률로서 규제하는 분할방식, ③규제의 대상을 특정하여 규제하는 개별방식 등이 있다.[17]

앞에서 살펴 본 바와 같이 미국은 Privacy Rule이라는 통합방식의 개인정보보호법률이 존재함에도 불구하고 HIPAA를 따로 제정하였다. 이는 의료정보가 개인정보의 일종임에는 틀림없으나 개인의 privacy와 관련하여 그 민감성이 상대적으로 매우 높은 까닭에 별도로 더욱 엄격한 보호를 목적으로 개별 법률을 제정한 것이다. 물론 HIPAA의 제정 목적은 개인정보보호에만 있는 것이 아니라 의료정보를 전산화함으로써 파생될 수 있는 민사절차, 형사절차, 행정절차, 조세절차 등의 특수성에 대해 일괄적 특례규정을 마련하기 위한 것도 있었다. 그러나 그 주된 제정 목적은 역시 의료정보의 보호를 더욱 엄격히 하기 위한 것이었음을 부인 할 수는 없다.

지금 우리는 개인정보보호 방식에 관하여 통합방식과 분할방식을 사이에 두고서도 합의를 이루지 못하고 있는 상황에서, 공적부문과 민간부문에 넓게 퍼져 있는 의료정보를 통합방식이나 분할방식으로 커버하기란 어려울 것으로 예상된다. 따라서 의료정보에 대해서만 특정하여 공적부문과 민간부분에 모두 적용되는 규제 법률을 제정하는 이른바 개별방식이 적절할 것으로 생각된다.

2. OECD권고 개인정보보호 8개 원칙을 반영한 의료정보보호 원칙 수립

17) 백윤철, 앞의 글, 400면.

개인정보의 보호를 위하여 OECD는 ①수집제한의 원칙(Collection Limitation Principle), ②정보정확성의 원칙(Data Quality Principle), ③목적명확성의 원칙(Purpose Specification Principle), ④이용제한의 원칙(Use Limitation Principle), ⑤안전보호의 원칙(Security Safeguards Principle), ⑥개인적 참여의 원칙(Individual Participation Principle), ⑦공개의 원칙(Openness Principle), ⑧책임의 원칙(Accountability Principle) 등 8개 원칙을 권고하였다.[18)]

이를 의료정보에 반영한다면, ①환자에 대한 당해 의료서비스와 직접 관련성이 없는 정보는 수집할 수 없고(수집제한의 원칙), ②환자가 부정확한 의료정보의 정정, 삭제 등을 요구할 수 있어야 하며(정보정확성의 원칙), ③환자에 대해 당해 의료정보의 사용 목적을 명확히 제시하고 가공처리정보가 임상연구 등의 다른 목적에 사용되어질 수 있음을 고지하는 동시에 고지된 목적을 벗어나는 사용을 할 수 없으며(목적명확성의 원칙), ④의료정보주체가 동의한 목적의 사용 이외의 다른 목적에 사용할 수 없으며(이용제한의 원칙), ⑤의료정보의 불법사용 또는 유출을 방지할 수 있는 시스템적 또는 제도적 안전장치를 마련하여야 하며(안전보호의 원칙), ⑥의료정보의 생성, 유통, 이용 등에 당해 정보주체의 개인적 참여가 보장되어야 하며(개인적 참여의 원칙), ⑦의료정보의 처리과정 및 사용주체 등에 대한 내용이 공개되어야 하며(공개의 원칙), ⑧의료정보의 관리주체는 위에서 언급된 원칙들이 준수될 수 있도록 필요한 조치를 강구하고 정보주체에 대한 침해가 발생할 경우 이에 대한 적절한 책임을 부담해야 한다.(책임의 원칙)

3. 안전보호원칙에 따른 시스템 설계의 가이드라인 제시

우선 의료정보의 통합시스템에 대한 대안을 먼저 제시하고 이에 대한 가이드라인을 살펴보기로 한다. 우리는 교육정보시스템(NEIS)의 구축과정에서 노출된 문제점들을 통하여 정보의 집적이 가져올 수 있는 파장을 이미 경험 한 바 있다. 막대한 예산을 투입하여 구축된 통합시스템이 지금은 저장적 기능만을 수행하는 통합서버가 한국교육학술정보원(KERIS)에 물리적으로 존재할 뿐, 사실상 기능은 각 급 학교 단위의 개별적 운영체제를 유지하고 있다. 처음부터 이러한 설계를 하였다면 사회적 파장도 막을 수 있었고 예산도 절감할 수 있었을 것이다. 따라서 의료정보시스템은 개별 의료기관 단위로 운영되는 것이 원칙이다. 다만, 자체적으로 시스템을 구축하기 어려운

18) 백윤철, 앞의 글, 401-402면.

영세한 의료기관들을 위하여, 병원들의 중복 투자비용을 절감하기 위하여, 또한 정보의 교류를 위하여 표준화된 시스템을 설계하고 물리적 저장서버만을 중앙에서 또는 지역 단위에서 구축하는 방법을 병용하자는 것이다. 다시 말해서 개별 의료기관은 국가적 차원에서 개발된 표준화된 시스템을 사용하여 개별적으로 SI(system integration)를 구축하되 개별 의료기관의 의료정보는 중앙 또는 몇 개의 지역 단위에 설치된 중앙 서버에 저장하는 방식을 추진하자는 것이다. 이러한 방식을 취할 경우, 개별 의료기관은 SI 설계비용과 서버 등의 인프라 구축비용을 절감할 수 있을 뿐만 아니라, 시스템이 표준화 되어 있으므로 의료기관간의 정보교류도 활성화될 수 있을 것이다. 이러한 시스템 하에서는 개별 의료기관의 의료정보는 원칙적으로 해당 의료기관에서만 액세스가 가능하며, 다른 기관에서 직접 액세스할 수는 없게 된다. 의료기관간 또는 의료기관과 건강보험공단 또는 보험회사간의 의료정보 교류는 정보주체의 동의나 요청에 의하여 암호화된 코드를 사용하여 전송하는 방식을 취하는 것이 바람직하다. 또한 당해 의료정보가 해당 기관에서 필요한 목적으로 가공처리 된 이후에는 해당 서버에서 자동으로 삭제되도록 설계하는 것도 필요하다.

다음으로, 표준화 시스템의 개발과 관련하여 또는 기존에 이미 개별 병원이 구축·운영하고 있는 시스템과 관련하여 설계상의 가이드라인을 제시할 필요가 있다. 대부분의 개별 의료기관이 구축하여 운영하고 있는 의료정보시스템은 환자의 인적정보와 진료기록정보가 한꺼번에 인식되도록 구축되어 있는 것이 일반적이다. 다시 말해서, 환자의 성명, 주민등록번호, 진료카드번호가 동시에 출력되는 방식으로 개발되어 있는 것이 일반적이다. 그러나 의료정보의 특수성을 고려한다면 환자의 인적정보와 진료기록정보가 분리 되도록 설계되어야 한다. 다시 말해서 주민등록번호 등에 진료기록정보 파일이 따라 붙는 방식을 지양하고, 별도로 부여 받은 환자의 고유 인식번호(일반적으로 진료카드 번호)에 진료기록 파일이 붙도록 설계되어야 한다. 모듈이 데이터를 액세스할 때 주민등록번호에는 환자의 인적정보만을, 진료카드 번호에는 진료기록정보만을 출력하도록 시스템이 설계되어야 한다. 이렇게 설계될 경우 원무과에서는 환자의 진료예약, 진료비용 징수 등의 업무를 처리함에 있어 환자의 인적정보만을 액세스할 것이며, 의사는 반대로 환자의 진료기록만을 액세스하고 인적정보는 접근할 수 없게 되는 것이다. 이미 의료정보시스템을 구축·운용하고 있는 경우에도 이러한 시스템의 설계변경에 그다지 많은 비용이 들어가지 않는 다는 것이 전문가의 의견이다. 따라서 이에 대한 가이드라인을 조속히 마련하여 이를 적용한 시스템이 구축될 수 있도록 해야 할 것이다.

김민호

의료정보(medical informations), 개인정보(personal informations), 미국의료정보보호법(HIPAA), 전자정보(electronic informations), 종이문서정보(paper information)

[abstract]

A Study on the Present State and Appropriate Direction for Legislation about Protection of Personal Medical Information

Prof. Kim, Min-Ho

Lots of large sized hospitals have already installed medical informations computing system. However, legislator and government have not made any policies and legislations for regulating and protecting privacy about personal medical informations. Of course, there are statues of privacy rule for protection of personal informations. If a term of medical informations is included in a term of personal informations broadly, present privacy rule could regulate use or disclosure of medical informations for privacy protection. But, medical informations are very sensitive informations compared with other personal informations. Therefore, the special privacy rule for regulating about protection of personal medical informations has to make as soon as possible. On this article, I suggest a appropriate direction for legislation about protection of personal medical informations according to analyzing into U.S.A.'s statute for privacy act about personal medical informations - "Health Insurance Portability and Accountability Act".