

정보화시대의 환자진료정보 보호에 관한 법·제도적 고찰

윤 경 일

계명대학교 의료경영대학원

<Abstract>

A Study on Medical Information Privacy Protection Law and Regulation in the Information Age

Kyung Il Youn

Graduate School of Healthcare Administration, Keimyung University

This study discusses the direction of legislation to strengthen the legal protection of medical records privacy in information age. The legislation trends on privacy protection of medical records in European Union and United States are analysed and the current law and regulation of Korea on medical records are compared. The issues discussed include the ownership of medical records, the patient's right of access to medical records, medical information publication for other than treatment or insurance processing use, confidentiality responsibility of provider organizations, medical information management in provider organizations, penalty for the unlawful use of patient information. This study concludes that the patients' right on medical record and provider organization's responsibility in processing patient information should be strengthened in order to protect patients' privacy and to conform to the international standard on medical record protection in the information age.

Key Words : Medical records, Privacy, Medical law, HIPAA, Information age.

I. 연구의 필요성

진료정보는 환자를 진료하는 동안 발생한 정보의 일체로 환자의 의료정보, 개인신상에 관한 자료, 재정적 자료 등 의료기관에서 환자진료를 위해 필요 사항을 문자화, 전자화, 사진화 하여 수집한 정보라고 정의할 수 있다 (손상영 등, 1998). 이러한 자료는 환자진료의 기초자료, 진료에 참여하고 있는 의료인간의 의사소통 수단 등 환자진료 목적 이외에 의료보험청구의 근거자료, 제공된 진료의 적정성, 합법성을 증거하는 법적인 자료, 보건의료의 연구나 교육의 기초자료 등 다양한 용도로 사용되어 그 공유의 필요성이 증대하고 있다.

진료정보 공유의 필요성 증가는 정보통신기술의 비약적 발전에 의한 의료정보의 전산화로 충족되고 있다. 전산화된 진료정보는 다수의 관계자에게 다량의 정보를 신속하게 전달하므로 환자에게 양질의 의료를 효율적으로 제공하는데 기여한다. 이러한 정보의 공유는 의료기관에서 환자대기시간의 단축, 불필요한 중복검사 감소, 환자정보 분석에 따른 증거에 의한 임상적 접근 (evidence based medicine), 신약의 개발 등 연구를 통한 의료의 질 적 향상과 의료 서비스 제공에 있어서 운영의 효율성을 도모하여 결국 국민의료비의 효과적 운용에 중요한 역할을 할 수 있다(통신개발연구원, 1995).

그러나 한편으로 진료정보의 전산화에 따라 다량의 개인정보가 수집, 보관되어 여러 관련 기관이 공유할 수 있게 되므로 환자의 사생활 보호 측면에서 여러 가지 새로운 문제점이 야기되고 있다 (Anderson, 2000). 진료정보에 대한 접근성이 향상됨에 따라 환자의 개인적 정보의 대량노출의 가능성이 높아지고 있으며, 환자 개인정보의 누출에 따른 부작용은 개인의 사생활 보호의 차원을 넘어 실질적으로 개인의 직장생활, 취업, 보험혜택, 금융기관 대출관련 등 개인의 경제생활에 직접적인 불이익을 초래할 수 있다. 동시에 보다 근본적으로는 개인정보 누출의 개연성이 증가함에 따라 환자와 의료제공자간의 관계가 손상될 가능성 또한 증가하게 된다는 것이다. 환자가 개인정보 누출에 대한 우려 때문에 자신의 건강상태에 대한 정보를 밝히지 않거나, 정확한 정보를 제공하는데 어려움을 느낀다면 이것은 의료전달체계의 기본 단위가 되는 환자와 의료제공자간의 관계를 훼손하는 경우가 된다. 환자와 의료제공자간의 관계 훼손은 진료의 효과성과 효율성에 치명적인 결과를 초래할 뿐 만 아니라 전염성 질환일 경우 사회전체에 주는 피해는 막대하다 할 수 있다.

따라서 진료정보의 전산화는 의료서비스 제공의 효율성 측면에서만 추진되어서는 안되며, 진료정보의 수집과 사용 과정에서 정보에 대한 환자의 권리를 강화하므로 환자의 사생활 보

호를 위한 법제도적 조치가 함께 보완되어야 할 것이다 (배대현, 2001). 진료정보보호에 대한 법제도적 조치가 일견 정보공유의 활성화에 악영향을 미칠 것으로 생각되기 쉬우나 장기적인 관점으로 보면 이러한 보호 조치가 미흡한 상태에서의 정보공유 활성화는 기대하기 어려울 것이다. 따라서 본 연구는 정보화에 따른 외국의 개인정보보호를 위한 법제도적 접근방향과 진료정보에 관한 입법현황을 분석하여, 현재 우리 나라의 법제도적 미비점을 개선할 수 있는 방안의 제시를 목적으로 한다.

II. 개인정보보호에 관한 외국의 법제도적 접근 방향

급속한 정보화에 따라 사생활권에 대한 기본시각이 소극적인 개념에서 적극적인 개념으로 변화하고 있다. 개인사생활권을 단순히 혼자 있을 수 있는 권리(the right to be let alone)에서 '정보주체가 자기에 대한 정보의 전파를 통제할 수 있는 권리'라는 적극적 개념으로 이해하게 된 것이다 (김유향, 2002; 전태수, 1992). 이러한 관점을 수용하여 European Union (EU)과 미국은 개인정보를 다루는 기관이나 기업의 개인정보 처리에 있어서 사생활 보호를 강화하기 위한 다양한 입법활동을 하고 있다. 이러한 미국과 EU의 정보화시대의 사생활보호를 위한 법제도 정비는 상호 비교가 되는 방향에서 접근하고 있는데, EU의 경우 정부주도로 포괄적이고 세부적인 규제를 추구하고 있는 반면에 미국은 적정수준의 정부 규제를 시행하나 해당 기업이나 기관의 자율적 규제를 강조하는 방향으로 접근하고 있는 것이다 (Klosek, 2000). 여기서 EU와 미국 및 일본의 접근 방향과 이들이 우리에게 주는 시사점을 검토해 보면 다음과 같다.

1. EU의 접근방법

EU에 소속된 각국은 70년대까지 개별적으로 사생활 보호관련 법제도를 구축하다가 1981년 유럽평의회(Council of Europe)에서 EU국가간 개인정보보호의 일관성을 유지하기 위하여 Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (Convention 108: 협약 108)를 정립하였고, 모든 국가는 이 기준에 적합한 방향으로 국내 법안을 개정하였다. 협약 108의 주된 내용을 보면 1) 일반적 개인정보의 관리기

준과 함께 '민감한 정보' (sensitive data)를 '인종적 정보, 정치나 종교 등에 대한 개인적 신념 및 건강과 성생활을 나타내는 정보'라고 정의하고 이러한 정보의 처리에 대한 적절한 법적 조치를 취할 것을 규정하였고, 2) 수집·저장되는 정보에 대한 개인의 알권리를 강화하여 정보 수집기관은 적정한 기간 내에 적정한 비용으로 정보주체의 정보접근권을 수용하도록 하였으며, 3) 개인의 부정확한 정보에 대한 수정을 요구할 수 있는 권리와 부정확한 정보에 의한 피해를 보상받을 권리를 보장하고, 4) 이러한 기준에 합당하는 법제도적 조치가 미흡한 국가와의 개인정보 공유를 제한한다는 것이다.

또한 EU는 1998년 10월에 협약 108의 내용을 강화하고 EU회원 국가간 정보공유 기준을 정하기 위해서 European Directive on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data (European Data Protection Directive: 유럽연합정보보호령)를 채택·시행하였다. 법령의 주된 내용을 보면 1) 국가별로 모든 산업에 적용되는 포괄적인 규제를 의무화하고, 포괄적 규제를 채택하지 않은 국가는 이를 채택한 국가와의 개인정보공유를 제한하였으며, 2) 개인정보의 수집과 사용에 강력한 규제를 명문화하였고, 3) 각 국가로 하여금 독립적인 사생활정보관리기관을 설립하여 개인자료를 수집, 복사, 송달할 때 사전에 이 기관에 등록을 의무화하고 있다. 따라서 EU이 외에 미국을 포함한 대부분의 국가들은 이러한 수준의 개인정보보호 조치를 취하지 못한 상태이기 때문에 정보의 교류에 제한을 받게 된다. 이에 대처하여 미국과 EU는 장기간의 협상을 통하여 Safe Harbors Program에 합의를 보고 개인정보를 교류하는 조직들이 이 기준을 따르도록 하므로 잠정적으로 유럽연합정보보호령의 정보공유제한 원칙의 적용을 유보하고 있는 상태이다 (이정원, 2001).

2. 미국의 접근방법

개인정보의 보호를 위한 미국의 접근방향은 기본적으로 국가는 개괄적인 입법을 통하여 개인정보보호에 관한 방향을 제시하고 구체적인 사항은 각 관련기관이 자율적으로 수행하도록 하는 것이다. 개인정보보호가 미흡하다는 EU의 지적에 대하여 미국은 일관되게 Federal Trade Commission에서의 규제로서 정부의 역할은 충분하다는 시각을 가지고, 개인정보를 취급하는 각 조직의 정보의 수집·사용에 관한 사항이 고객에게 피해를 유발 할 경우 결국은 소비자의 저항에 의하여 해당 사업을 추진할 수 없게 된다는 논리로 시장 선택적인 개인정보 취급 자율규제의 정당성을 주장하고 있다(Klosek, 2000). 또한 정부는 개인정보를 취급

하는 조직들이 개인정보보호에 문제가 지속적으로 발생하는 경우에도 불구하고 적절한 조치를 취하지 않을 시 정부가 직접적인 규제조치를 취할 것이라는 입장을 산업계에 분명히 하고 있다고 주장하고 있다.

EU가 요구하는 개인정보보호 강화를 위한 여러 조치들 중 특히 개인이 자신의 정보에 대하여 무제한적인 접근권을 갖는 것에 대하여 미국정부는 이러한 조치가 조직에게 과도한 비용적 부담이 된다는 이유에서 반대하고 있다. 이러한 EU와 미국간의 개인정보보호에 대한 기본시각의 차이는 단시간내에 해소될 수 없을 것으로 전망되어 임시적으로 Safe Harbors Program에 기준하여 유럽과 미국간의 개인정보 교류가 유지되고 있는 실정이다.

3. 일본의 접근방법

일본의 경우 개인정보는 통신보호에 관한 여러 법률, 즉 통신사업법, 유선통신법 등에 의해서 보호를 받고 있다. 그러나 미국의 접근방향과 같이 민간부문을 대상으로하는 개인정보 보호에 관한 포괄적인 입법은 없으며, 정부지침 및 고시와 민간의 자율규제에 의존하고 있는 상황이다. 다만 개인의 사적정보 보호를 위한 지침을 마련하여 신용 및 의료정보 등 정보의 누출에 따른 피해가 큰 분야에 대한 규제방안을 명문화하기 위해서, 1999년 8월 부정한 방법으로 통신망 등에 접근하는 행위 (컴퓨터 네트워크의 해킹 등)를 금지하는 법안인 「부정접근행위의금지등에관한법률」이 의회에서 통과되어, 2000년 2월부터 시행되고 있다(이정원, 2001)

4. 시사점

진료정보는 EU의 협약108에서 규정하는 '민감한 정보'에 속한다고 볼 수 있으므로 일반적인 개인정보와 구별하여 법제도적인 보호조치를 할 필요가 있다. 또한 우리나라에서의 의료정보에 대한 환자의 권리인정 수준은 적극적인 인정을 추구하는 EU와 비교적 소극적인 미국간에 상호합의한 Safe Harbors Program의 기준을 따르는 것이 타당할 것으로 사료된다. 그 이유로 Safe Harbors Program은 개인정보의 보호에 있어서 EU와 미국 양측의 중간 정도의 법제도적 강도를 보이고 있고, 이러한 기준에 따라 EU와 미국간의 개인정보 교류에 있어서의 장애가 극복되었다고 볼 수 있기 때문이다. 의료정보에 대한 개인의 권리관련에 대한 이러한 접근은 2003년 4월부터 미국이 제정 시행하고 있는 HIPAA (Health Information

Portability and Accountability Act)의 예에서도 볼 수 있다 (Rada, 2003; Hussong, 2000). 따라서 우리 나라의 의료정보보호를 위한 조치는 환자와 의료기관의 입장을 고려하여 Safe Harbors Program에서 지정하고 있는 기준에 합당한 방향으로 법제도를 정비하므로 사회적 비용을 최소화할 수 있는 수준에서 진료정보의 보호와 국제적인 개인정보 교류에 필요한 기준을 만족할 수 있을 것으로 사료된다.

Ⅲ. 진료정보보호 관련 국내외 법제도 현황

1. 진료정보의 소유권

1) 개념정립

진료정보의 소유권에 관한 개념의 확립은 진료기록을 작성한 의료기관과 정보의 대상이 되는 환자의 진료기록에 관한 의무와 권리를 정하는 기본시각 설정하기 위하여 필요하다 (Batami, 2001). 미국의 경우 진료기록의 물적 형태(문서 테이프, 필름 등) 소유권은 그 정보를 작성한 의료기관에 있는 것으로 인정되고 있다. 의료기관의 진료기록 소유권을 인정하는 논리적 근거는 (1) 진료기록은 의료인간의 의사소통 수단으로 환자진료 지속성확보를 위한 주요 수단이 되며, (2) 진료기록에 기록된 자료는 의료종사자들의 진료의 질 보장, 평가, 및 향상을 위한 연구에 필요한 정보를 제공하고, (3) 의료기관의 진료수행에 대한 증거가 되어 보험청구를 위한 기본자료이며, (4) 법적인 자료로서 의료의 거래에 있어서 의료인과 환자를 동시에 보호하는 역할을 하기 때문이다. 그러나 이러한 의료기관의 진료기록에 대한 물적 소유권은 그 매체가 포함하고 있는 환자정보의 내용에는 적용되지 않는다. 즉 의료기관이 소유하고 있는 환자정보에 대한 물적 소유권이 보장되지만 그 물적 매체에 있는 환자정보의 내용의 소유는 환자에 속하는 것으로 보아 환자의 진료기록에 대한 접근을 허가하는 개념적 근거가 된다.

2) 외국의 사례

진료정보 소유권에 관한 입법 예는 미국 오하이오 주법에서 의사나 치과의사의 의무기록에 관련하여 환자를 진료하면서 생성된 기록은 의사 본인의 사용을 위해서 작성된 것이며

따라서 의사의 개인적 소유물로 간주한다는 규정에서 볼 수 있다. 보다 적극적인 의료기관의 진료기록 소유권의 인정의 예로는 오하이오 주법에서 개원의가 의원을 타 의사에게 명도하였을 경우 이러한 명도가 의사의 가구, 집기 등과 함께 매도하는 의사의 영업권도 명도하는 것으로 보아 진료기록도 같이 명도할 수 있도록 정하고 있다.

3) 국내 법제도 현황 및 문제점

우리 나라의 경우 진료기록의 소유권을 명시한 법조항은 존재하지 않고 다만 의료법제21조(진료기록부등)에 진료기록의 기록보존의무를 명시하고 있으며, 동법 시행규칙 제18조는 각 문서별 보관기간이 명시되어 있으며 시행규칙 18조 제4항과 제5항은 폐업의 경우 진료기록부를 보건소에 이관하거나 관할보건소장의 허가를 받아 개인이 소유할 수 있도록 하고 있다.

따라서 진료기록의 소유권에 대한 조항을 명시하므로 진료기록의 소유권적 성격을 규명하여 의료기관은 진료기록의 관리에 대한 책임을 가짐과 동시에 이를 환자진료 및 보험행정에 사용할 권리를 보장하고, 환자에게는 자신의 의료정보에 대한 접근권을 확보할 수 있는 근거를 마련하여 진료정보의 사용 및 관리에 따르는 법제도적 근거를 마련할 필요가 있는 것으로 사료된다.

「의료법」

제21조 (진료기록부등)

①의료인은 각각 진료기록부·조산기록부·간호기록부 그밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)을 비치하여 그 의료행위에 관한 사항과 소견을 상세히 기록하고 서명하여야 한다. [개정 2002.3.30.] [[시행일 2003.4.1.]

②의료인 또는 의료기관의 개설자는 진료기록부등(제21조의2제1항의 규정에 의한 전자기록부를 포함한다. 이하 제33조제2항에서 같다)을 보건복지부령이 정하는 바에 의하여 보존하여야 한다. [개정 75·12·31, 87·11·28, 97·12·13 법5454, 2002.3.30.] [시행일 2003.4.1.]

「의료법시행규칙」

제18조 (진료에 관한 기록의 보존)

① 의료기관의 개설자 또는 관리자는 진료에 관한 기록을 다음 각호와 같이 보존하여야 한다. [개정 93·8·20, 2000·6·13]

1. 환자의 명부 5년 2. 진료기록부 10년 3. 처방전 2년 4. 수술기록 10년 5. 검사소견기록 5년 6. 방사선사진 및 그 소견서 5년 7. 간호기록부 5년 8. 조산기록부 5년 9. 진단서등 부분(진단서·사망진단서 및 시체검안서등 별도 구분하여 보존할 것) 3년

⑤ 제4항의 규정에 불구하고 폐업하는 의료기관의 개설자는 진료기록의 종류별 수량 및 목록·보관장소·보관책임자등을 기재한 진료기록보관계획서를 제출하여 관할보건소장의 허가를 받아 자체보관할 수 있다. [신설 94·9·27] [전문개정 90·1·9]

2. 환자의 진료정보 열람

1) 개념정립

70년대 초까지만 하여도 환자의 진료기록열람권은 상당히 제한되고 있었다. 이러한 제한의 배경은 (1) 의사들의 진료기록공개에 대한 부정적인 태도, (2) 진료기록의 공개가 의사와 환자간의 관계에 부정적인 영향을 주리라는 우려, (3) 진료기록의 공개가 초래할 환자의 정서에 대한 부정적 영향, (4) 기록이 공개될 경우 그 기록의 정확성에 대한 시비로 인한 의료분쟁의 소지 등이다. 이러한 이유에서 제한되어오던 진료기록의 공개가 1980년대에 들어오면서 이를 공개하는 방향으로 전개되었다. 이러한 방향전환의 이유를 보면 (1) 정보화 사회에서 진료기록에 수록된 정보의 내용에 대한 환자의 알권리의 인정, (2) 진료정보가 제3자에게 주어졌을 때 자신에게 어떤 영향을 줄 것인가에 대한 환자의 주관적 판단의 존중, 3) 진료기록 공개를 통한 의료공급자에 대한 환자의 신뢰성 확보, (3) 환자 자신의 건강상태에 대한 인지를 통한 환자의 건강회복에 긍정적인 영향, (4) 치료의 질이나 환자기록의 질 적 향상에 기여, 마지막으로 (5) 의료기관 서비스에 대하여 환자가 비용을 지불하였으므로 자신의 진료기록에 접근의 정당성 인정 등의 이유에서이다. 이러한 진료기록 열람에 대한 시각의 변화는 정보화시대의 개인정보 보호에 대한 적극적 해석에 기인한다고 볼 수 있다.

2) 외국의 사례

미국 오하이오 주법(RC 3701.74(C))에 의하면 의료기관은 환자진료 종료 후 30일내에 진료 기록의 최종본을 작성하여야 하며, 환자가 진료기록을 검토하고자 할 때 서명된 문서를 의료기관에 제출하면 의료기관은 진료기록을 공개하도록 하고 있다. 그러나 환자를 진료한 의사가 명확한 이유에서 요구된 진료기록을 공개함이 환자에게 불리한 결과를 초래할 것이라는 결정을 하면, 의료기관은 환자에게 직접공개하지 않고 환자가 지정하는 의사에게 의무기록을 제공하도록 하고 있다.

한편 미네소타주법 (144.335 Subd.2. Patient access)은 환자의 진료기록 열람권을 더욱 자세히 명시하고 있는 바 의료공급자는 환자의 요구에 응하여 환자의 진단, 치료, 및 예후에 대한 정보를 완전하고 최근성이 보장된 내용으로 일반환자가 이해할 수 있는 용어를 사용하여 제공하여야 한다고 규정하고 있다. 또한 예외로 규정한 경우를 제외하고 의료공급자는 환자의 열람요청에 대하여 적절한 비용으로 신속히 정보를 제공하여야 하는 바 공개내용은 환자의 상태를 진단하기 위하여 생성된 검사결과보고서, x-ray, 처방전, 및 기타 기술적 정보를 포함한 내용 등이다. 열람을 거부할 수 있는 정보는 의료제공자가 작성한 환자의 건강상태에 대한 문서화된 추측(speculation)이나 특정 정보가 공개될 때 환자의 육체적 정신적 건강에 해가되거나 타인을 해할 가능성이 있다고 정당하게 판단할 경우, 또는 아동에 대한 육체적 학대, 성적 학대에 대한 비데오테이프의 복사본 등에 대한 열람을 거부할 수 있다고 규정하고 있다.

또한 AMA (American Medical Association)와 ADA (American Dental Association)는 내부의견서를 통하여 환자의 의무기록 접근권을 인정하고 있는 바 환자의 적절한 동의가 있을 때 현재 환자를 진료하고 있는 의사의 요구에 따라 환자의 의무기록이 제공되어야하며, 환자나 다른 의사가 요청하고 환자의 향후 진료에 유용하다면 환자의 진료정보를 공개해야한다는 원칙을 정하고 있다 (AMA, 2001).

3) 국내 법제도 현황 및 문제점

우리 나라의 경우 「의료법」 20조에 환자 기록열람 등에 관한 규정이 있으며, 동법 18조의 2 처방전 발부에 관한 사항에서 환자가 진료기록을 열람할 수 있는 경우를 규정하고 있다. 그러나 기록열람 등에 관한 조항은 환자의 정보열람권을 보장한다는 시각보다 기본적으로는 열람을 제한하고 열람을 허용하는 경우가 예외적인 경우로 기술되어 있으며, 동법 제20조 2

항의 진료기록 송부에 대한 사항도 그 기본적인 시각이 의료전달체계의 효율성 확보라는 의도에서 제정된 것으로 적극적인 의미에서 환자정보의 열람권 보장의 의도는 제시되지 않고 있다고 할 수 있다. 또한 환자에 대한 정보의 제공이 허용되지 않는 경우를 '치료목적상 불가피한 경우'로 모호하게 지정하므로 의료인이나 의료기관의 의도에 따라 '치료목적'을 넓게 해석하므로 기록열람을 적극적으로 제한할 소지가 있다.

「의료법」

제20조 (기록 열람등)

①의료인 또는 의료기관 종사자는 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 환자에 관한 기록의 열람·사본교부 등 그 내용확인예 응하여서는 아니된다. 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 응하여야 한다. [개정 87·11·28, 94·1·7, 2000·1·12]
[시행일 2000·7·13]

②제1항의 규정에 불구하고 의료인은 동일한 환자의 진료상 필요에 의하여 다른 의료기관에서 그 기록·임상소견서 및 치료경위서의 열람이나 사본의 송부를 요구한 때 또는 환자가 검사기록 및 방사선필름등의 사본 교부를 요구한 때에는 이에 응하여야 한다. [신설 94·1·7]

③의료인은 응급환자를 다른 의료기관에 이송할 때에는 환자인송과 동시에 초진기록을 송부하여야 한다.

제18조의2 (처방전의 작성 및 교부)

①의사 또는 치과의사는 환자에게 의약품을 투여할 필요가 있다고 인정하는 때에는 약사법에 의하여 자신이 직접 의약품을 조제할 수 있는 경우를 제외하고는 보건복지부령이 정하는 바에 의하여 처방전을 작성하여 환자에게 교부하거나 발송(전자처방전에 한한다)하여야 한다. [개정 2002.3.30.] [시행일 2003.4.1.]

3. 진료정보의 정정

1) 개념정립

현대 정보화 사회에서의 개인의 사생활권은 '자기에 관한 정보를 관리, 통제할 수 있는 권리'까지 포괄하는 적극적 개념으로 파악(자기정보통제권)되고 있다. 따라서 개인이 자기에 관한 정보를 언제, 어떻게, 어느 정도 타인에게 유통시키느냐를 스스로 결정하는 권리(자기정보결정권)로서 프라이버시 개념이 이해되고 있다. 이렇게 볼 때 온라인상에서 보호대상이 되는 환자정보는 각 개인이 자신에 관한 정보의 공표 여부를 결정할 뿐만 아니라 더 나아가 수집된 정보의 내용을 정정, 삭제하는 권한까지 포함한다고 볼 수 있다. 이러한 정보정정에 대한 환자의 권한은 정보화시대에서의 의료정보공유 상에 발생하는 의료정보의 훼손의 가능성이 높아진 환경에서 특히 중요하다고 할 수 있다 (Campbell 등, 1997).

2) 외국의 입법현황

미국의 HIPAA규정은 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. 진료정보의 정정을 요구받은 의료인이나 의료기관은 이러한 요구에 대하여 60일 이내에 타당한 조치를 취해야 한다. 다만, 정정요구된 내용을 당해 의료인이나 의료기관이 수집, 작성하지 않았을 경우, 정정요구된 정보를 검토하기 위하여 접근할 수 없을 경우, 정정요구된 정보가 정확하고 완전할 경우 등에는 진료기록의 정정을 거부할 수 있도록 하고 있다(Redhead, 2003; Rada, 2003).

3) 국내 법제도 현황 및 문제점

우리 나라 「의료법」 상에는 진료기록의 정정절차에 대한 규정이 없고 「공공기관의정보공개에관한법률」에 처리정보의 정정에 관한 내용이 명시되어 있다. 그러나 동 법의 적용대상은 제2조(적용대상)에 명시된 바와 같이 대통령이 정하는 기관으로 제한되고 있으며 이 법에 근거한다면 의료기관 중 적용대상은 대학교에 부설되어 있는 대학병원급 의료기관이 해당하므로 그 적용대상이 제한적이다. 따라서 의료정보의 수집과정에서의 오류, 정보의 저장, 유통 시 발생할 수 있는 정보의 변조 등에 따른 부정확한 정보에 의한 환자에 대한 피해를 방지하기 위하여 환자에게 정보정정 요구권을 부여하고 이에 대한 절차를 명시할 필요가 있다.

「공공기관의정보공개에관한법률」 (1996)

제2조 (적용대상) 법 제2조제1호에서 "대통령령이 정하는 기관"이라 함은 다음 각호의 기관을 말한다. 이 경우 제2호 및 제3호의 규정에 의한 기관에는 금융실명거래및비밀보장에관한법률 제2조제1호의 규정에 의한 금융기관은 포함되지 아니한다. [개정 97·12·31, 98·4·1, 99·1·29]

1. 초·중등교육법 및 고등교육법 기타 다른 법률에 의하여 설치된 각급 학교
3. 특별법에 의하여 설립된 특수법인

제14조 (처리정보의 정정) ①제12조의 규정에 의하여 본인의 처리정보를 열람한 정보주체는 보유기관(다른 기관으로부터 처리정보를 제공받아 보유하는 기관을 제외한다. 이하 이 조에서 같다)의 장에게 서면으로 당해 처리정보의 정정을 청구할 수 있다.

②보유기관의 장은 제1항의 규정에 의한 정정청구를 받은 때에는 처리정보의 내용의 정정에 관하여 다른 법률에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체없이 이를 조사하여 필요한 조치를 한 후 그 결과를 당해 청구인에게 통지하여야 한다.

③보유기관의 장은 제2항의 규정에 의한 조사를 함에 있어 필요한 때에는 당해 청구인으로 하여금 정정청구사항의 확인에 필요한 증빙자료를 제출하게 할 수 있다.

4. 진료정보의 제3자 공개

1) 개념정립

진료정보는 환자 진료를 위한 목적과 함께 의과학, 병원경영, 보건행정 등 학문적인 연구에도 중요한 기초자료가 된다. 진료정보의 전산화와 함께 이러한 목적에서의 정보에 대한 접근의 요구가 급증하고 있다. 제3자에 대한 환자정보 공개는 개인을 식별할 수 있는 정보공개와 식별자료가 삭제된 상태로의 정보공개로 나눌 수 있다. 개인식별이 가능한 정보공개인 경우 환자의 동의 여부를 공개의 조건으로 하는 것이 일반적이고 개인식별자료가 삭제된 상태의 자료는 제한 없이 공개되어 학문적 연구에 사용할 수 있도록 하는 것이 타당할 것으로 사료된다.

2) 외국의 입법현황

미국의 HIPAA는 의료기관이 환자와 환자의 대리인 이외의 제3자에게 의료정보를 환자의 동의없이 제공할 수 있는 경우로 정보의 공개 목적이 치료나 보험청구를 위한 것이거나 개인식별 자료가 삭제된 정보로 한정하고 있다. 즉 진료정보 생성의 원래 목적 수행을 위하여 정보가 공개될 경우 환자 동의가 필요하지 않으나, 그 이외의 목적으로 환자 개인을 식별할 수 있는 정보가 공개될 때는 환자의 동의를 득하도록 명시하고 있다. 또한 환자개인을 식별할 수 있는 정보의 경우 정보사용 목적을 수행하기 위한 최소한의 정보만 공개할 것을 명시하고 있으며, 환자 정보공개동의서에 정보공개의 목적, 범위, 기간 등을 명시하여 동의를 득할 것을 규정하고 있다. 그러나 환자 개인을 식별할 수 없는 정보의 경우 그 유통에 대한 규제는 거의 없고 다만 개인신상을 나타낼 수 있는 항목을 명시화하여 이러한 정보가 제거되어야 공개할 수 있도록 정하고 있다.

HIPAA 규정은 환자 개인을 식별할 수 있는 변수로 전화번호, 팩스번호, 전자우편주소, 사회안전번호, 의무기록번호, 피보험자번호, 구좌번호, 면허번호, 차량번호, 의장번호, 웹URL, 인터넷 IP주소, 지문이나 음성인식 등 생물학적 인식정보, 인물사진, 또는 개인인식이 가능한 기타 고유번호나 특성 및 코드로 정하고 있다. 한편 유럽연합정보보호령은 개인식별이 가능한 정보공개 조건을 정보의 대상이 명시적인 동의를 보였을 때, 정보의 대상이 육체적으로 또는 법적으로 명시적인 동의를 할 수 없으나 정보공개가 환자의 안녕을 위하여 중요할 때, 정보의 대상이 정보를 스스로 공개하였을 때로 규정하고 있다(Redhead, 2003; Rada, 2003).

3) 국내 법제도 현황 및 문제점

「의료법」 제20조는 환자의 진료목적을 위한 의료기관 간의 진료정보 공유를 허용하고 있으나 기타 목적에 대한 언급이 없으며, 실제로는 다른 의료기관이나 환자가 의료기록을 요구할 때 다양한 이유로 이 조항은 잘 지켜지지 않고 있는 것이 현실이다. 「공공기관의개인정보보호에관한법률」에서는 정보의 제3자 공개에 대한 내용을 명시하고 있으나 앞에서 언급한 바와 같은 적용범위에 문제가 있다. 또한 동법에서 명시하고 있는 공공기관이 수집해 보유하고 있는 개인정보를 활용함에 있어서, 정보주체의 동의를 요하지 않는 '상당한 이유'의 범위에 관하여 상당한 논란이 있다(한국통신정책연구원, 2003).

「의료법」

제20조 (기록 열람등)

②항 ③항 「공공기관의개인정보보호에관한법률」

제10조 (처리정보의 이용 및 제공의 제한)

①보유기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니된다.

②보유기관의 장은 제1항의 규정에 불구하고 다음 각호의 1에 해당하는 경우에는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있다. 다만, 다음 각호의 1에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다. [개정 99·1·29]

5. 진료정보의 기밀누설 금지 대상자

1) 개념정립

환자진료기록은 의료기관의 대형화, 의료서비스의 분업화에 따라 의료인 뿐 만 아니라 의료기관내 약사, 기사 등 진료보조 직원, 보험심사, 병원기획, 원무 등의 업무처리를 담당하는 행정관련 직원 등 의료기관에 종사하는 거의 모든 사람이 환자정보를 업무상 사용하고 있다. 따라서 이러한 환경의 변화에 맞추어 현행의 의료인으로 국한되는 환자기밀누설 의무의 대상자가 확대되어야 할 것으로 사료된다(손상영 등, 1997).

2) 외국의 입법현황

미국의 HIPAA에서는 환자정보보호관련 규정의 적용대상자를 의료보험사, 의료관련 행정처리 센터 및 각급 의료기관으로 HIPAA의 표준에 의하여 마련된 정보를 전자매체를 통해서 송신하는 개인 (의사, 간호사, 치과의사, 약사, 물리치료사 등), 조직 (병원, 검사센터, 앰블런스 회사 등), 또는 그룹(연합클리닉 등)으로 명시하여 환자정보보호 의무를 부과하고 있다 (Redhead, 2003; Rada, 2003).

3) 국내 법제도 현황과 문제점

현행 「의료법」 19조는 환자정보에 대한 기밀 보장 의무를 의료인에게 제한하고 있다. 의료인은 의료법 상 의사, 간호사 및 조산사로 규정되고 있으므로, 기밀보장 의무 적용 대상을 의료인을 포함한 관련 종사자 및 의료기관으로 확대할 필요가 있다.

「의료법」

제19조 (비밀누설의 금지) 의료인은 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료·조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못한다.

6. 진료정보 기밀보호 책임자의 임명 및 조직 내 교육

1) 개념정립

환자 진료정보의 전산화와 의료서비스의 다양화 및 복잡화로 인하여 진료정보의 보호는 더 이상 의료기관의 특정 종사자나 일부 부서의 업무에 국한될 수 없다. 즉 진료정보의 보호는 의료기관 전체를 대상으로 하는 정책적 사안이 되는 것이다. 따라서 각 의료기관은 환자정보보호에 대한 정책을 수립하고 이를 시행하며, 필요에 따라 대상 직원을 정기적으로 교육하고, 인적, 시스템적 문제점의 보완을 추진할 수 있는 조직과 인력을 갖출 필요가 있다.

2) 외국의 입법 현황

미국의 HIPAA 규정은 의료기관이 사생활보호담당자를 지명하여 사생활보호정책수립, 직원교육, 정보보호, 불만사항 접수, 사생활보호규정 위반자에 대한 제재 등의 업무를 수행하도록 하여야 한다고 규정하고 있다(Redhead, 2003; Rada, 2003).

3) 국내 법제도 현황과 문제점

의료기관내 환자정보가 업무상 또는 업무외적으로 많은 사람들에게 접근가능하며, 특히 정보화와 함께 의도적 또는 비의도적으로 정보의 대량 유출 및 훼손이 가능하게 된 상황에서 정보의 체계적인 관리가 필요한데도 불구하고 이를 전담하여 체계화 할 수 있는 인력이 정

해져 있지 않아 정보관리에 대한 책임소계가 불분명하고, 일괄적인 정보관리 정책이 부재한 형편이다. 현재 「의료법」에서는 이러한 규정을 두고 있지 않고 있으므로 정보화사회에서 환자정보를 체계적으로 관리하기 위해서는 이러한 규정의 신설이 필요할 것으로 사료된다.

7. 벌칙규정

1) 개념정립

정보화사회의 도래에 따라 환자정보의 보호가 중요한 사안으로 조명되고 있는 바 이러한 환경의 변화와 정보보호 중요성의 적극적 인식을 위해서 의료정보의 훼손, 변조, 불법이용에 관한 벌칙규정을 명확히 규정하여 이러한 행위의 사전예방과 정보처리에 있어서의 환자정보 보호의 중요성을 강조할 필요가 있다.

2) 외국의 입법 현황

미국의 HIPAA 규정은 의도적으로 환자정보보호에 관한 HIPAA 규정을 어겼을 경우 50,000불 이하의 벌금, 또는 (그리고) 1년 이하의 징역을 부과하고, 사취를 목적으로 거짓 증언한 경우 100,000불 이하의 벌금, 또는 (그리고) 5년 이하의 징역, 상업적 이득이나 개인적 이득, 또는 악의적으로 해할 목적으로 개인을 식별할 수 있는 진료정보를 매매, 이전, 또는 사용할 경우 250,000 이하의 벌금, 또는 (그리고) 10년 이하의 징역을 부과하도록 명시하고 있다(Redhead, 2003; Rada, 2003).

3) 국내 법제도 현황과 문제점

[의료법] 제67조 (벌칙) 제68조 (벌칙) 제69조 (벌칙) 조항에 포괄적으로 벌칙을 규정되어 있으나 환자정보의 오·남용을 사전에 예방한다는 차원에서 벌칙조항을 명확히 제시할 필요가 있는 것으로 사료된다.

IV. 결 론

우리 나라 「의료법」을 살펴보면 근본적으로 진료정보의 보호와 관련된 직접적인 규정은

의료법 제19조 의료인의 기밀누설금지조항과 18조2의 제3항 전자처방전에 저장된 진료정보에 관한 사항 정도라고 볼 수 있다. 그 밖의 진료기록관련 규정은 환자진료정보의 보호라는 시각에서보다는 의료기관 운영 기본지침이나 의료전달체계의 운용에 있어서의 효율성 확보 차원에서의 규정으로 볼 수 있다. 의료법의 이러한 문제점은 정보화시대의 환경적 요구를 담아내지 못하고 있는 것으로 사료되므로 환자정보보호와 정보에 대한 환자의 적극적 권리를 보장하는 방향으로 법령을 보장하여야 할 것이다.

의료정보의 전산화는 근본적으로 의로서비스 제공상의 질 향상과 효율성의 향상이라는 두 가지의 목표를 가지고 진행되어야 한다. 이러한 목표는 환자의 개인정보에 대한 통제권을 부여하는 적극적인 방향으로 법적 제도적 환경이 뒷받침 될 때 달성될 수 있다. 의료정보공유의 활성화와 환자개인정보의 보호는 일견 상반되는 개념으로 이해될 수도 있으나 의료정보의 생성, 관리, 공유, 폐기 등의 과정에서 개인정보의 보호가 투명하게 제도화 된 기반 하에서만 의료정보공유의 활성화가 달성될 수 있는 것이다. 의료에 있어서 가장 기본적인 단위는 의료인과 환자의 관계이며 이 관계에 있어서 기밀성이 보장될 때만이 환자가 의료제공자에게 자신의 건강상태에 대한 정확한 정보를 제공 할 수 있으며, 의료정보의 전산화가 이러한 기밀성을 훼손하게 된다면 진료의 질에 악 영향을 미칠 뿐만 아니라 결국 수집되는 정보의 질 또한 보장할 수 없게 될 것이다.

환자의 진료정보에 대한 적극적인 권리보장은 환자들에게 자신들의 정보에 대한 접근권, 정정요구권, 자신의 정보의 사용 및 공개에 대한 알권리의 보장 등의 조치에 의하여 실현될 수 있다. 진료정보에 대한 환자의 권한을 적극적 인정하는 것은 세계적인 추세이며, 정보화 시대에 이러한 추세에 적응하지 못할 경우, 국가간 정보교류에도 불이익이 초래될 수 있는 것이다. 이렇게 볼 때 진료정보에 대한 환자의 권리보호는 미국과 EU간의 합의에 의하여 설정된 Safe Harbors Program의 기준을 따라 설정하는 것이 타당하다고 본다.

개인정보의 보호에 관한 미국의 자율 규제적 접근과 EU의 포괄적 정부규제방식의 접근은 양측의 갈등관계를 가져왔고, EU가 European Data Protection Directive를 제정·시행함에 따라 미국과 EU소속 국가들간의 개인정보 공유에 많은 제한이 따르게 되었다. 이러한 문제점을 해결하기 위하여 미국과 EU는 2년간의 협상기간을 거쳐 잠정적으로 Safe Harbors Program의 타결을 보게 된 것이다. 따라서 Safe Harbors Program은 개인정보보호에 있어서 미국과 EU간의 중간정도의 강도로 개인정보를 보호하는 원칙으로 볼 수 있고 이것이 결국에 국제적인 표준이 될 가능성이 있다. 또한 미국은 Safe Harbors Program에서 규정하는 내용을 수용하는 수준에서 HIPAA를 제정 시행하여 의료정보보호를 제도화하고 있다. 따라서

우리 나라의 의료정보보호관련 법이 국제적으로 받아들여 질 수 있을 만한 수준을 확보하기 위해서는 최소한 Safe Harbors Program의 기준을 충족시킬 수 있는 법적 조치가 필요할 것으로 사료된다.

이러한 의미에서 Safe Harbors Program에서 규정하고 있는 개인정보 보호를 위한 7대 원칙을 보면 첫째, 고지(Notice)의 원칙으로 개인정보를 취급하는 조직은 정보의 주체에게 개인정보 수집의 목적, 정보이용에 대한 정보주체의 질문 및 불만사항의 신고절차, 정보를 공유하는 제3자의 성격, 정보공개에 대한 정보주체의 권리 등을 정보주체에게 고지하고, 둘째, 선택(Choice)의 원칙으로 정보주체가 자신의 정보가 정보수집의 원래 목적과 다르게 사용될 수 있는지 여부를 선택할 수 있는 권한부여하며, 셋째 제공(Onward Transfer)의 원칙으로 정보수집자가 제3자에게 정보를 제공할 경우 고지와 선택에 대한 의무가 제삼자에게도 적용된다는 원칙과 넷째, 안전성 (Security)의 원칙으로 정보의 생성, 유지, 이용 또는 보급하는 조직이 정보의 오용, 불법적 접근, 공개, 훼손으로부터 보호하기 위한 합리적 조치를 취할 의무 다섯째, 정보 무결성(Data Integrity)의 원칙으로 정보의 사용목적에 필요한 범위 내에서 정보의 원래 목적에 부합하는 사용, 정확성, 안전성, 최신성을 보장하는 합리적 조치를 취할 의무이며 여섯째, 접근(Access)의 원칙으로 정보주체는 자신의 정보에 대한 접근권을 가지고 정보의 내용이 부정확하다면 비용이나 부담이 프라이버시권 침해에 비하여 크지 않고, 타인의 프라이버시권을 침해하지 않는 범위 내에서 정정이나 삭제를 요구할 수 있는 권리의 인정 및 일곱째 집행(enforcement)의 원칙으로 제시된 원칙이 준수되지 않을 경우 정보의 주체가 갖는 권한, 원칙을 준수하지 않은 조직에 대한 책임을 확인할 수 있는 기전의 마련 등을 천명하고 있다.

따라서 이러한 개인정보보호에 관한 원칙을 수용하는 방향으로 진료정보보호를 위한 법안이 마련되어야 할 것이다. 또한 법제정의 방법으로는 개인사생활보호차원에서 의료정보의 중요성을 고려할 때 의료정보보호 관련 특별법도 생각해 볼 수 있지만 이것이 여의치 않을 경우 적어도 의료법 내에 독립된 장을 설정하여 입법하는 것이 타당할 것으로 사료된다.

참 고 문 헌

김유향(2002). 온라인프라이버시. 입법정보 제60호.

배대현(2001). 냅스터 사례에서 드러난 인터넷상 정보공유의 한계. 산업재산권 제10호.

손상영, 윤지웅(1998). 인터넷의료정보서비스 확산에 대비한 보건의료정책의 개선방안. 한국통

신정책연구원.

손상영, 윤지웅, 김혜경(1997). 의료정보 서비스 개선을 위한 법·제도 정비, 한국통신정책연구원.

이정원 (2001). 전자거래와 개인정보보호에 관한 연구. 석사학위논문. 고려대학교 대학원.

전태수 (1992). 고도정보화 사회에 있어서 공공기관의 개인정보보호에 관한 연구. 석사학위논문. 고려대학교 정책과학대학원.

통신개발연구원(1995). 초고속 정보통신기반구축 관련 법제도정비연구 (보충자료I). 통신개발연구원.

한국통신정책연구원(2003). 미, 단계별 개인정보 보호법안 발의. Center for Law & Information Society.

AMA(2001). Report 4 of the Council on Medical Service: Medical care online.

Anderson, JG(2000). Security of the distributed electronic patient record: a case-based approach to identifying policy issues. International Journal of Medical Informatics.

Batami S (2001). Patient data confidentiality and patient rights. International Journal of Medical Informatics 62.

Campbell, SG, Gibby, GL, Collingwood, S(1997). The internet and electronic transmission of medical records, Journal of Clinical Monitoring. 13.

Hussong, SJ(2000). Medical records and your privacy: Developing Federal Legislation to Protect Patient Privacy Right. American Journal of Law and Medicine 26.

Klosek, J(2000). Data Privacy in the Information Age. Quorum Books, 2000.

Rada, RR(2003). HIPAA@IT Reference, 2003: Health Information Transactions, Privacy, and Security. Health Information and Management Systems Society.

Rada, RR, (2003). Privacy and Health HIPAA 2003. Health Information and Management Systems Society

Redhead, S.C(2003). Medical Records Privacy: Question and Answers on the HIPAA final rule, CRS Report for Congress.