

전자의무기록(EMR)의 활용과 환자정보보호

전영주‡

조선이공대학교 보건의료행정과

EMR System and Patient Medical Information Protection

Youngl-Ju Jeun‡

Department of Health Administration, Chosun College of Science & Technology

<Abstract>

The purpose of this study is to find out the most successful way for the protection of medical information focusing on the electronic medical record(EMR). In this study, every aspect of the EMR is reviewed in terms of the hospital management. In particular, definitions, major functions, strengths and weaknesses of the EMR are considered. This study also examines the general development of the EMR as well as the current situation of applying the EMR. Important issues such as the protection of patient Medical information, informed consent, and the customer-oriented hospital information system are discussed and interpreted in light of the introduction of the EMR into the area of the hospital management. Finally, in this paper Protection of medical information by major Issues on Patient medical information

Key Words : Medical Information, Protection of Medical Information, EMR System

‡Corresponding author(jun@cst.ac.kr)

I. 서론

최근 의료업계의 환경은 의료기관의 영리법인 허용과 약약분업 실시, WTO DDA 협상에 의한 의료서비스 시장 개방의 추진 등으로 인해 경쟁이 더욱 심화될 것으로 보인다. 또한 소비자의 의식수준이 높아지고 보다 양질의 의료서비스를 요구함에 따라 의료기관은 급격한 외부환경에 맞춰 마케팅 활동을 활발히 수행할 것을 요구하고 있다[1]. 환자가 병원을 방문하여 가장 먼저 행하는 것이 응급환자의 경우 응급처치가 우선이지만 대부분의 환자들은 접수창구를 통하여 개인신상정보를 요구받게 된다. 즉, 통상적으로 병원 진료는 원무과 등에서 환자의 인적사항 등의 작성부터 병원의 진료가 개시되는 것이 일반적이다. 이러한 환자의 개인정보를 바탕으로 의사는 객관적 검사와 의사의 주관적 판단에 의해 진단이나 처방 등의 처치를 시행하게 된다. 또한 이러한 환자의 의료정보가 진료기록지에 작성되고, 보관되어 의사의 진료, 의학적 연구, 보건정책자료, 법적소송, 건강보험청구 등 많은 개인적 또는 공익적 자료로 매우 광범위하게 활용되고 있다.

EMR(Electronic Medical Record)이란 정보기술의 급격한 발달, 컴퓨터의 다양한 기능 수행, CD-ROM이나 DVD같은 정보 저장 매체의 발달 등 과학의 급속한 변화에 따라 이제까지 종이에 기록하던 환자의 진료기록을 컴퓨터를 활용한 전자적 형태의 의무기록을 지칭한다. 또한 최근에는 언제 어디서나 서비스 이용이 가능한 유비쿼터스 기술의 등장으로, 의료 서비스 역시 질병 발생 후 대응하는 병원 중심 치료 패러다임에서 탈피하여, 병원이 아닌 환자의 집, 사무실 또는 이동 중에도 의료서비스를 받을 수 있는 u-헬스케어 서비스 연구가 활발히 진행되고 있고, 원격진료를 통한 장소적 제약 없이 보다 양질의 진료서비스를 이용할 수 있는 시대가 되었다. 즉, 다양한 유무선 네

트워크를 통하여 수집된 생체 및 환자의 의료정보가 교환 될 뿐만 아니라 다양한 접근 경로를 통해 의료기기 및 시스템을 제어 할 수 있고[2], 건강정보를 이용한 의료 서비스에 따라 다양한 정보 소비자가 발생 및 개입 될 수 있다. 그러나 EMR을 비롯한 다양한 헬스케어 서비스 구조는 보안상 취약성과 공격에 노출 될 위험이 크다. 특히, 네트워크에서 발생 및 교환되는 정보는 극히 개인적인 건강정보, 생활 습성, 신체적 특징 등과 같이 프라이버시에 민감한 정보들이 대부분이고 거주자의 건강과 생명에 연관성이 있는 민감한 정보들이 대부분으로서 서비스에서의 정보보호는 안전하고 신뢰성을 보장하기 위한 방안이 필수적으로 고려되어야 한다. 이에 병원에서도 의무기록의 EMR의 도입에 따른 종이진료 차트는 사라지는 추세이고, 그에 따른 네트워크 통합화와 환자의 의료정보관리의 중요성이 점점 부각되고 있다. 또한 정보화 사회가 급속도로 진행되고 개인정보가 광범위하게 수집되고 관리되는 상황에서 개인의 사생활의 보호를 위하여 소극적인 비밀의 유지뿐만 아니라 자신에 대한 정보를 본인이 직접 관리하고 통제할 필요성이 커짐으로서 자기 자신에 대한 정보를 자율적으로 결정하고 관리할 수 있는 권리가 사생활의 비밀 및 자유 또는 프라이버시의 중요한 내용으로 포섭되게 되었다. 이러한 권리를 일반적으로 '개인정보자기결정권'이라고 한다. 이는 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 다만, 우리 헌법은 개인정보자기결정권에 대하여 명시적으로 규정하고 있지는 않지만 학설과 판례는 일반적으로 헌법 제10조의 인간의 존엄과 가치 및 행복추구권에 근거를 두고 있는 일반적 인격권, 제17조의 사생활의 비밀과 자유 그리고 제37조 제1항의 헌법상 열거되지 아니한 기본권 조항 등에서 개인정보자기결정권을 도출하고 있다. 따라서 개인정보 중 환자의 의료정

보는 가장 민감한 정보이고 프라이버시보호가 강조되어야 할 정보이며, 이러한 정보의 침해는 명백한 헌법상 개인정보자기결정권을 침해한다[3]. 또한 환자의료정보의 불법적 유출은 과거 불법행위 이론을 통한 권리구제로는 한계가 있으며 보다 근본적 보호대책이 시급하다. 병원의 의료정보보호와 관리를 위해서는 가장 먼저 선행되어야 할 문제가 의무기록 관리에 대한 중요성의 인식이다. 의무기록은 의료관계종사자가 필수적으로 작성하는 기록으로 의료기관에서 관리하고 보관된다. 의무기록의 작성자는 주로 의료인 등의 의료종사자로 이들 종사자의 정확한 의료기록의 작성 및 관리가 중요하다. 본 논문에서는 EMR의 활용 과정인 수집, 저장, 이용, 타인에게 자료제공 및 환자정보의 파기 단계를 세분화 하여 발생할 수 있는 문제를 비교법적·해석론적 연구방법으로 환자의 의료정보 보호를 위한 법적·정책적 대안제시를 그 목적으로 한다.

II. 이론적 배경

1. 전자의무기록(EMR)의 개념

전자의무기록은 한 개인의 전 생애에 걸친 건강상태와 의학적 문제가 전자화된 형태로 유지되는 정보의 총체이다. 전자의무기록의 영어 명칭이나 개념정의를 각국마다 아직까지 통일되어 사용되고 있지는 않고 있다. 미국의학협회에서는 전자의무기록의 정의를 "정확한 자료를 제공하고 의료인에게 필요한 정보를 주어 임상결정을 도와주기 위한 병원정보시스템이나 처방전달시스템 내부에 포함되어 있는 전자적 형태의 환자기록"이라고 정의하고 있고, 미국의 의무기록연구소(Medical Record Institut; MRI)는 "중이매체에 기록되어 시행되었던 모든 의료기록을 그 업무처리 구조나 정보의 범위, 정보 내용에 있어 변함없이 동일하게 전산화를 통

해 업그레이드시킨 디지털화된 형태"를 말한다. 환자의 진료행위를 중심으로 발생한 업무상의 자료나 진료 및 수술, 검사기록을 약속된 코드 등 활용 가능한 형태로 전산에 기반 하여 입력, 정리, 보관하며 입력된 자료를 통해 의사소통을 하는 시스템을 통칭한다고 정의하고 있다. 또한 미국의 의학연구소(Institute of Medicine; IOM)는 전자의무기록을 "안전하고 정확한 자료와 여러 가지 의학지식에 기초한 의사결정을 지원해주는 전문가시스템을 가진 전자형식의 의무기록"이라고 정의하고 있다. 또한 Lehman Broth에 따르면 전자의무기록은 "환자의 의무기록지에 포함된 의사의 처방 내용과 또 다른 형식으로 기술된 내용을 전산매체에 저장하여 저장된 의료정보를 컴퓨터를 통해 사용자가 더욱 쉽게 접근하고 통합할 수 있도록 지원하는 시스템"으로 정의하고 있다[4]. 전자의무기록으로 표현되는 EMR은 단순히 과거의 의무기록을 자동화한 형태가 아니라 다양한 정보매체의 형태로 건강에 대한 모든 정보를 함축하고 있다. 그러므로 전자의무기록에는 개인의 병력, 현재의 투약상태, 검사결과 등의 건강정보를 쉽게 입력하고, 저장하며, 사용자들이 이용하기 편리한 형태로 처리하여 제공되고, 사용자간에 정보 교환을 용이하게 하며, 정보 안정성을 모두 제공할 수 있어야 한다. 또한 권한을 부여 받은 사람만이 전자의무기록에 쉽게 접근할 수 있어야 하고 정확하고 완전한 환자정보, 환자 특수 상황에 대한 경고 시스템, 임상적 의사결정 지원, 의학 참고자료의 연결, 공중보건 및 보건정책 자료의 활용 등에 이용되는 환자의 중요한 개인정보의 총체로서 정보보호의 필요성이 무엇보다 중요하다.

2. 전자의무기록(EMR)의 법적근거와 환자정보

전자의무기록의 법적근거는 의료법 제22조2의 규정(진료기록부 등)에 의한다. 제22조2의 규정은

‘의료인이나 의료기관 개설자는 진료기록부등(전자 의무기록 포함)을 보건복지부령으로 정하는 바에 따라 보존하여야 한다.’라고 규정되어 있고, 규칙 제15조에 진료에 관한 기록의 보존을 규정하고 있고, 진료기록부는 10년 기간 동안 보존하여야 한다. 라고 규정하고 있다. 제23조의2(전자의무기록) 「①의료인이나 의료기관 개설자는 제22조의 규정에 불구하고 의무기록부 등을 전자서명법에 의한 전자서명에 기재된 문서(이하 “전자의무기록”이라 한다)로 작성·보관할 수 있다. ②의료인이나 의료기관 개설자는 보건복지부령이 정하는 바에 따라 전자의무기록을 안전하게 관리·보존하는데 필요한 시설 및 장비를 갖추어야 한다. ③누구든지 정당한 사유 없이 전자의무기록에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다.」고 규정하고 있다. 기존 의료법 제21조에서 종이 진료기록부와 마이크로필름 또는 광디스크 등만을 인정하고 있고, 전자의무기록은 임의 수정, 변조가 가능하기 때문에 법적효력을 갖지 못한 것으로 제한되던 상황에서 진일보하였다. 병원에서 기록되는 환자 정보는 개인정보 중 가장 민감한 정보이다. 의료정보를 구체적으로 분류하면 주관적 정보, 객관적 정보, 가치판단적 정보로 구별할 수 있다. 주관적 정보는 정보의 주체인 환자에 의해 발생하는 극히 개인적인 개인정보이다. 객관적 정보는 검사, 진료 등의 결과를 기록지 등에 기재된 정보를 말하며, 가치판단적 정보는 의료인이 환자가 제공하는 주관적 정보와 검사 및 진료 등을 통해 얻어진 객관적 정보를 바탕으로 의사의 전문성에 기초하여 작성된 정보를 말한다. 또한 객관적 정보를 바탕으로 생성된 자료를 2차 의료정보 또는 가공의료정보로 표현되기도 한다. 주관적 정보는 환자에 의해서 기록되는 문서이므로 적절한 방식으로 작성, 수집, 수정되어야 하며, 정당한 사유 없이 개인의 의료정보를 탐지하거나 유출, 변조되어서는 안 된다. 그리고 연구결과정보나 의학

정보는 환자가 제공하는 주관적 정보와 객관적 정보를 바탕으로 이루어진 정보이기 때문에 개인정보자기결정권을 기초로 보호 받을 법익이 있다. 다만, 공공의 이익 내지 공적 필요에 의해서만 제한적으로 관계자의 동의하에 열람 등이 가능하다고 판단된다. 무엇보다 중요한 것은 의료정보의 원천은 정보를 제공한 대다수 국민이며 의료종사자(의사 등)또한 의료기관을 이용한 국민의 의료정보(1차 의료정보 제공자의 자료)를 바탕으로 2차 의료정보가 생성된다고 보아야 한다. 따라서 국민이 의료기관을 이용하여 생성된 의료정보가 자칫 유출되었을 경우에는 여러 가지 심각한 사회적 문제로 발생될 가능성이 높으므로, 개인정보보호에 중요성이 높다고 할 수 있다.[5] 헌법 제17조에서 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.”고 규정하여 사생활의 비밀과 자유 또는 프라이버시권을 보장하고 있고, 제16조(주거의 자유), 제18조(통신비밀의 자유)를 통해서 사생활의 비밀과 자유의 구체적인 범위에 대해서만 보장하고 있을 뿐, 개인정보자기결정권의 헌법상의 근거가 무엇인지에 대하여 서론에서도 설명한바와 같이 학설 및 판례가 일치하지 않고 있다. 다만 헌법재판소 최근 판례에서 개인정보자기결정권의 헌법상 근거로 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문에서 일반적 인격권과 제17조의 사생활의 비밀과 자유로 판단하기도 하고, 헌법상 열거되지 아니한 독자적으로 기본권으로 이해되기도 하여 아직 일치된 견해를 보이고 있지 않다[6]. 또한 2012년 개정 생명윤리법에서는 유전정보를 ‘인체유래물을 분석하여 얻은 개인의 유전적 특징에 관한 정보’로 정의하고, 인체유래물을 ‘인체로부터 수집하거나 채취한 조직·세포·혈액·체액 등 인체 구성물 또는 이들로부터 분리된 혈청, 혈장, 염색체, DNA, RNA, 단백질’로 정의한다. 즉, 생명윤리법은 유전정보에 2차적 정보가 포함됨을 명확히 하였다고 할 수 있다. 또한 동법에서는 ‘개인정

보'를 별도로 정의하고 있는데, 이에 의하면 개인 정보는 '개인식별정보, 유전정보, 건강에 관한 정보 등 개인에 관한 정보'를 의미한다[7]. 그렇다면 생명윤리법상의 개인정보 개념은 개인정보보호법상의 개인정보나 진료정보, 건강정보를 모두 포괄하는 개념으로 해석할 수 있어 개인의 유전정보나 임상정보가 대량으로 집적하고 있는 바이오뱅크는 연구자들이 효율적으로 질병 자료에 접근할 수 있도록 하여 관련 의학 연구를 발전시킬 수 있는 장점이 있는 반면, 개인의 프라이버시를 크게 침해할 우려 또한 존재한다.

3. 환자 의료정보보호의 필요성

환자의 의료정보는 신체와 관련하여 전문적이면서 민감한 특성을 지니고 있고, 이를 타인에게 공개하거나 제3자에게 제공하는 것은 1차적으로 개인의 사생활에 대한 비밀과 자유라는 헌법상의 기본권에 대한 침해로 간주될 수 있는데, 이 외에도 인간의 존엄과 가치, 행복추구권과 같이 인간의 본질을 구성하는 기본권적 권리에 대한 침해를 가져올 수 있다. 특히 전자적 형태의 의무기록인 EMR은 복제 및 전송이 용이하여 유출되거나 위·변조된 정보가 확대 재생산될 경우 개인의 사생활이 침해될 가능성이 기존의 종이 형태로 보관되던 환경에 비해서 훨씬 높다[8]. 의료정보시스템의 구축은 필연적으로 의료정보의 공유를 통해 사생활 침해 가능성이 높다고 할 수 있으므로 이에 대한 보호의 필요성도 증대된다. 특히 환자의 의료정보가 EMR을 활용한 DB의 축적과 네트워크의 발달로 인해 다수의 의료관계자 및 연구자들에게 정보의 오·남용은 사생활에 중대한 침해는 물론 2차적 피해가 발생할 가능성이 높다.

4. 의료정보의 성질과 활용

의료정보의 법적 성질을 보면 특별하게 보호되는 개인의 내밀한 영역에 속하는 '민감한 정보'라고 할 수 있다. 따라서 의료정보는 일반 개인정보 중에서도 가장 보호법익이 강한 정보라고 할 수 있고, 고대 히포크라테스 선서에서도 환자의 비밀을 의료인 등이 윤리적 1차 덕목으로 준수해야 하며 보호되어야 하는 특성을 갖고 있다. 따라서 일반 개인정보와는 달리 민감한 정보로서 그 수집과 처리에서 매우 엄격한 제한을 받아야 하며, 의료인 및 기타 관계인에게 의료법 등에서도 비밀유지의무를 부여하고 있다[9]. 의료정보의 활용에서도 최근에는 유전자 검사 등을 활용한 범죄수사나 친자 확인, 인류학과 고고학 등 그 활용대상범위가 점차 확대해가고 있고, 신규직원의 건강기록을 채용과정에서 제출서류로 요구하고 있고, 채용 후에도 통상적으로 정기적인 건강검진기록을 요구하거나 검진 결과가 인사담당자로부터 알려지는 일들도 빈번히 발생되고 있다. 최근에는 보험회사에서도 의료정보를 활용하여 보험자의 면책을 주장할 수 있는 근거자료를 확보하기 위하여 의료정보가 활용되고 있고, 의료기관과 정부기관에서도 의료정보를 활용한 각종 통계조사와 연구, 정책 활용을 위한 자료로 활용되는 특성을 가지고 있어 의료정보가 잘못 유출되거나 가공되었을 경우 심각한 문제가 발생된다고 본다.

5. 전자의무기록(EMR)과 환자정보보호 현황

1) 국내

우리나라에서 전자의무기록(EMR)과 관련된 환자 정보보호에 관한 것은 의료법 및 보건의료정보법제를 포함하고 있다. 또한 헌법을 최상위법으로 하고 이를 근간으로 민·형사법, 보건의료관련법, 정보통신관련법 등 여러 개별 실정법에서 관련 조항들을 규정하여 규율하는 방식을 갖추고 있다. 전자의무기록(EMR)에 법적근거는 위에서 언급하였

음으로 환자의 정보보호와 가장 밀접한 법률은 개인정보 보호와 관련된 정보통신망이용촉진 및 정보보호 등에 관한 법률과 공공부문의 개인정보 보호에 관한 법률, 신용정보보호에 관한 법률 등이 있어 공공부문과 민간부분이 과거 나뉘어져 있어 실효성이 떨어졌으나 공공기관의 개인정보보호에 관한 법률이 개인정보보호법으로 전면 대체 입법(2011.3.29. 제정, 2011.9.30 시행)되어 모든 의료기관에 적용될 수 있게 됐다. 그 밖에 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 개인정보 보호 가이드라인(500명상 이상 의료기관 대상)'을 제정·공포하여 2010.3.15일부터 시행하고 있다. 그러나 개인정보 보호에 관한 개별 적용이 세분화되어 있어 자칫 법의 사각지대가 발생할 수 있어, 개인정보 보호 중 특히 정보의 특수성을 갖는 의료정보에서의 개인정보 보호는 취약할 수밖에 없다 [10][11]. 개인정보에 관해 의료기관을 포함한 모든 보건의료분야에 특정해서 적용하기 위한 일반법인 개인건강정보보호법(가칭)의 입법 작업이 2006.10월부터 추진되고 있고, 쟁점은 보건의료정보의 공유 또는 공동 활용으로 인해 얻을 수 있는 사회적 편익과 그에 따른 개인의 프라이버시 침해발생 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, 보건의료기초법에서 정의하고 있는 넓은 의미에서의 보건의료정보까지를 포괄하는 것이 타당하며, 특히 미래의 의료환경 변화를 예측하고 과학의 발달과 더불어 더욱 진화할 수 있는 원격의료 또는 U-health 시대를 대비해서라도 의료정보가 정보통신망을 통해 언제 어디서나 공유될 수 있다는 점을 감안해 환자의 정보보호를

위한 정확한 폐해를 파악하는 것이 법제화의 선결 과제라 판단된다[12].

2) 일본

일본에서 전자의무기록(EMR)은 '전자카르텔'이라는 명칭을 갖고 있다. 일본 보건의료복지정보시스템공업회는 전자카르텔을 5단계의 수준으로 구분하여 정의하고 있다. 1단계는 의료기관내 개별 부문 내에서의 전자화된 환자정보 공유화 단계이며, 제2단계는 의료기관내 복수의 부문간의 전자화된 환자정보 공유화 단계, 제3단계는 1개의 의료기관 내에서 환자의 호소, 증상, 치료계획 등의 환자정보 공유화 단계이며, 제4단계는 복수의 의료기관을 연결하여 상호 이용하는 형태의 환자정보 공유화 단계, 제5단계는 의료정보뿐만 아니라 보건후생성도 취급하는 공유화 단계를 지칭한다. 일본은 2003년 5월 민간부분에 대한 개인정보보호법이 제정되어 2005년 4월 1일부터 전면적으로 시행되고 있다[13]. 환자정보를 위한 노력은 1980년 OECD의 '프라이버시 보호와 개인 데이터의 국제유통에 대한 가이드라인에 관한 이사회 권고'에서 제시한 OECD 개인정보보호 8원칙에 영향을 받아 제도적 법안이 실행되고 있다.

3) 미국

미국의 경우 보건의료정보에 관한 연방특별법이 제정되기 이전에 개인 정보에 관련된 법률에 기초하여 보건의료정보를 보호하였고, 연방법의 제정 이후에도 개인정보 관련 법률은 여전히 중요한 역할을 하고 있다. 이와 관련된 대표적인 연방의 개인정보법은 1974년의 프라이버시법(Privacy Act, 1974)과 컴퓨터통합 및 프라이버시보호법(Computer Matching and Privacy Protection Act, 1988)이 있고, 이외에도 공정신용경리법(Fair Credit Bilding Act, 1976), 가족의 교육권 및 프라이버시에 관한 법률(Family Educational Rights

and Privacy Act, 1976), 공정한채무수집집행법(Fair Debt Collection Practices Act, 1977), 금융프라이버시에 관한 법률(Right to Financial Privacy Act, 1978), 전자통신프라이버시법(Electronic Communications Privacy Act, 1986 등이 있다[14]. 미국의 경우 보건의료기록은 일찍부터 주법에서 상호 상이한 수준에서 보호하고 있는데, 정보화가 가속화됨에 따라 주사이에 보건의료정보의 이전과 그 표준화가 문제되었다. 따라서 보건의료정보에 대한 통일법이 논의 되었고, 그 시도가 '통일보건의료정보법(Uniform Healthcare Information Act; UHIA)'의 제정으로 나타났다. 이와 같은 모델법에 의한 입법방식은 여전히 주법이라는 차원에서 한계를 지니고 있다. 그래서 연방정부는 연방차원의 실체법을 제정하였는데, 이것이 '1996년 건강보험의 이전과 책임에 관한 법률(Health Insurance Portability and Accountability Act; HIPAA)'이다. 이 법은 연방제도에서 나타나는 입법의 불일치를 해소하고 보건의료정보에 대한 통일된 규율이 필요한 사항에 관련한 법적 기반을 마련하였다는 점에서 중요한 의미가 있다.

미국의 의무기록연구소는 전자의무기록(EMR)의 발전단계를 5단계로 구분하여 설명하고 있다. 제1단계는 의무기록 자동화(automated medical record)단계이다. 이 단계의 자동화는 현재 병원에서 부분적으로 행해지고 있다. 보험급여비용의 청구를 위해 전산화 작업을 하거나 환자 관리를 위해 등록 등의 절차에 컴퓨터를 이용하는 수준이다. 제2단계는 의무기록의 전자보관(computerized medical record system)단계이다. 이것은 종이의무기록의 보관 공간 문제를 해결하기 위해서 도입된 방식으로, 단순히 의무기록을 사진으로 찍어서 컴퓨터에 보관함으로써 저장 공간을 절약하였다는 것 이상의 의미는 거의 없다. 제3단계는 전자의무기록(electronic medical record: EMR)의 단계이다. 의무기록을 활용이 가능한 형태로 보관하고 일단

의사의 처방이 내려지면 그것을 확인하고 고쳐지지 않도록 하는 하부구조를 갖고 있다. 병원 내에서 의무기록 전산화를 위해 개발·사용하는 시스템이며, 아래의 CPR보다는 협의의 개념이라고 할 수 있다. 제4단계는 전자의무기록시스템(computer-based patient record: CPR)단계이다. 이 시스템은 기존의 의무기록보다 광범위한 정보를 담고 있으며, 위 EMR 단계의 연장선상에 있다. 이 시스템을 가동하기 위해서는 전 EMR 체계의 국가적인 표준이 설정되어야 하고 상호 호환이 가능하여야 한다. 이 단계에서부터 의무기록을 원격의료에 적극 활용할 수 있다. 제5단계는 전자건강기록(electronic health record: EHR)단계이다. 전자건강기록은 가장 이상적인 단계로서, 이 단계의 의무기록에는 환자의 의료정보뿐만 아니라 민간의료 및 국가수준의 건강문제에 대한 모든 사항이 포함될 수 있다[15].

III. 결론

1. 환자 정보수집단계

환자의 의료정보를 수집하는 단계에서는 개인적인 민감 정보가 포함되어 있기 때문에 수집·이용의 목적, 항목, 기간 등에 대해서 정보주체에게 알리고 동의를 얻어야 한다(개인정보보호법 제15조). 특히 개인의료정보의 경우에는 정보주체의 동의나 다른 법률에 수집이 허용된 경우에만 예외적으로 수집할 수 있도록 하고 있으므로(개인정보보호법 제23조), 의료기관이 개인의료정보를 수집·이용하는 경우에 민감 정보로서 수집의 제한이 있고, 반드시 정보 주체의 동의를 얻어야 한다. 정보주체의 동의가 없는 수집이라면 환자의 정보보호권의 침해라고 볼 수 있다. 또한 동의가 단순한 동의가 아닌 충분한 설명의무를 이행한 후에 이에 대해 명확히 이해하고 결정을 내릴 수 있는 정보주체의

동의(Informed Consent)에 의해 정보를 수집하여야 하고, 설령 동의가 있다고 하더라도 정보주체의 동의에 위배된 정보 수집은 그 효력이 없다고 할 것이다. 흔히 의료기관에서의 동의절차는 정보주체의 입장에서 볼 때 만약 이러한 동의에 불응하면 의료기관 또는 의료기관 종사자로부터 불이익을 받을 것이라는 심리적 불안감이 작용할 수 있다. 이러한 심리적 상태에서 본인의 의사와 다르게 동의하는 경우에 원칙적으로 적법한 동의라 할 수 없다. 그러나 불안감을 느끼게 된 원인이 의료기관 등의 위력에 의한 것인지, 또는 정보주체의 선입견에 따른 것인지를 구분하여, 전자의 동의 의사표시는 당연히 무효이다. 이에 반해 후자의 경우 당연히 무효라 할 수는 없고, 동의의 철회 의사표시를 통해 동의의 효력이 철회의 의사표시 이후로는 미치지 아니하는 것으로 해석하는 것이 타당하다[16]. 그리고 개인정보수집에 관한 동의서와 수술동의서 등을 한 장에 같이 받도록 하는 것은 포괄적 동의에 해당하는 지에 대한 문제가 발생할 수 있다. 물론 이 경우에도 정보주체가 동의를 해야 할 항목을 명확하게 인지할 수 있어야 하고, 각각의 개별 항목에 대해 별도의 동의를 받도록 한다면 포괄적 동의에 해당한다고 할 수 없다. 따라서 환자의 동의와 정보 제공의 주체로서 자기에 대한 정보가 기록시스템에 어떻게 입력되어 있는가를 알 권리, 즉 자기정보에 대한 접근권(Access권)을 가지고 있으며(개인정보보호법 제35조), 또 그 정보가 잘못 되었을 경우 수정 내지 삭제 청구권을 행사(동법 36조)할 수 있어야 한다고 본다. 더불어 정보기록의 오류를 제거하기 위해서 자기정보에 대한 열람·복사권이 인정되어야 한다. 미래의 잠재적인 이용 예를 들어 의학연구 내지 보건정책적 연구라는 공익적 목적의 이용에 대비하여 편의성 내지 효율성이라는 관점에서 환자로부터 사전 동의를 받아놓는 것이 바람직한가라는 문제에 직면해서도 전자의무기록(EMR)의 생성단계에서부터 미리 자

료의 이용가능성에 대한 설명과 함께 이용에 대한 동의를 받아놓는 방법을 취하거나 전자적 형태의 환자의 동의를 구하는 방법을 강구하는 것도 가능하다. 환자에게 정보이용에 대한 충분한 설명과 아무런 외압이나 강압 없이 행하여진 동의의 경우에만 그 효과를 발휘할 수 있다. 따라서 병원에서 관행적으로 수행되는 정보이용에 대한 동의는 환자의 충분한 이해와 설명 없이 행하여진 경우 사후 적법한 동의가 아닐 수 있어 비진의 의사표시로 무효가 될 수 있으므로 정보의 수집단계에서부터 철저한 준비가 요구된다.

2. 환자 정보의 저장 및 이용단계

환자 정보의 저장 및 이용단계에서 발생하는 문제는 크게 두 가지로 구분할 수 있는데, 첫째, 이용목적의 범위를 넘어선 의료행위 또는 학술연구 등의 목적으로 이용되는 경우와 둘째, 이용목적과는 관계없이 금전적 이익이나 개인의 친분을 통해서 의료기관에 저장되어 있는 개인의료정보를 제공하거나 알려주는 경우이다. 첫째의 경우에 이용목적의 범위를 넘어선 경우라도 환자를 위한 의료행위로서 긴박한 사유가 있거나 환자가 당연히 동의를 했을 것이라 판단할 수 있는 경우에는 적법한 행위로 인정될 수 있다. 그러나 연구·학술목적의 이용의 경우에는 정보주체에 대해서 수집과정에서 동의를 얻지 못한 경우에는 목적 외의 이용이 된다. 따라서 이러한 이용에 대해서는 원칙적으로 적법하지 못한 이용이라고 할 것이다. 특히, 전자의무기록(EMR)의 경우에는 의료인들 간에 시간적으로 제약 없이 동시에 여러 장소에서 접근할 수 있고 정보를 공유하거나 교류할 수 있다는 점에서 효율성의 장점을 가지고 있다. 결정적인 자료가 부족하기는 하지만 적정한 의료라는 의료의 질 향상도 도모할 수 있다는 점, 그리고 임상연구, 역학조사, 보건의료통계의 기초자료로서 국가적 차

원에서도 활용가능한 과학적 근거자료가 될 수 있다는 장점도 가지고 있다. 하지만, 전자의무기록(EMR)이 상용화되어 정착하기 위해서는 의료기관 간의 의무기록 시스템의 통합이 필요하며 이를 위해 의무기록 표준화 작업, 개인정보 보호를 위한 제도적 대책 수립 및 보안유지의 안전성을 확보하기 위한 시설 및 장비의 구축도 전제되어야 한다 [17]. 오늘날 의료정보는 병원정보화(HIS: hospital information system)가 급속히 진행되고 있고, 보협전자청구시스템(EDI: electronic data exchange), 처방전달시스템(OCS: order communication system) 등의 정보자동화를 넘어 원격의료(Telemedicine), U-Health(ubiquitous), 모바일원격의료(M-Telemedicine) 등의 출현은 환자에게는 많은 편리성 및 유용성을 가져다 줄 수 있지만 반대로 의료정보 위협에 더욱 쉽게 노출시킬 수 있는 문제점도 함께 가지고 있기 때문에 의료정보의 안전성 및 신뢰성을 담보할 수 있는 시설 및 장비의 제도적 표준화가 시급하다. 둘째의 경우 금전적 목적 및 개인의 친분을 이용하여 환자의 민감 정보를 유출되는 사례가 늘어나고 있다. 이러한 문제를 해결하기 위해서는 정보관리자의 철저한 윤리의식이 필요하다. 정기적으로 정보관리자 및 병원직원들의 교육을 통해 윤리의식을 확보하고, 의료기관 내에서도 정보를 접근할 수 있는 권한을 엄격히 제한하여 정보 통제를 위한 의료기관의 제도적 보완이 필요하다.

3. 환자 정보의 보유와 파기단계

점점 의료정보가 전산화되고 네트워크화 되고 있어 무엇보다 중요한 것이 철저한 보안이다. 따라서 보안을 강화하기 위한 주기적인 패스워드 관리, 접근자의 허용 등급 조정, 보안점검 등의 업무 프로세스가 필요하다. 또한 의료정보 보안시스템에서 발생할 수 있는 문제점으로는 첫째, 의료 환경의

급격한 정보화로 인한 네트워크 환경구축과 인터넷 등을 활용한 공간적 제약의 축소는 해킹에 위협성, 물리적인 기계결함 등에 의해 언제라도 타인에게 의료정보가 유출될 수 있는 문제를 내포하고 있어 의료정보의 비밀성, 무결성 유지에 어려움을 줄 수 있다. 둘째, 의료정보가 경제적 가치가 생긴 다거나 잘못 처리된 의료정보는 의료정보의 수정 변질의 문제가 발생된다. 셋째, 의료정보의 도난이나 저장된 정보의 삭제 및 정전, 홍수 등의 재해가 발생할 경우 의료정보를 적절히 활용 가능한 가용성에 문제가 된다. 따라서 정보보안 시스템이 일반적으로 갖추어야 할 요소인 비밀성, 무결성, 가용성을 유지·발전시킬 수 있는 시스템 구축이 필요하다[18][19]. 환자 정보의 파기와 관련하여, 개인정보보호법 제21조 제1항은 “개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 법령에 따라 보존하여야 하는 경우에는 그러하지 아니한다.”고 규정하고 있다. 전술한 바와 같이 진료 정보를 수집할 때 환자로부터 별도의 동의를 얻은 경우에 있어서는 당해 정보의 보유기간에 대하여 고지하고 동의를 얻도록 하고 있다. 즉, 의료법 제22조 제2항은 “의료인이나 의료기관 개설자는 진료기록부(전자의무기록(EMR)포함) 등을 보건복지부령으로 정하는 바에 따라 보존하여야 한다”고 규정하고 있으며, 이에 따라 의료법 시행규칙 제15조는 진료기록부의 경우 10년을 보존하여야 한다고 규정하고 있다. 그런데 의료법은 이와 같이 의무보존기간은 정하고 있으나, 이 기간이 경과한 후에는 아무런 규정을 두고 있지 않다. 이에 따라 의료기관들은 10년의 의무보존기간이 경과한 후에도 실무상 이를 계속보유하고 있는 경우가 현실적으로 많다. 의료법 시행규칙 제15조 규정의 해석은 10년의 의무보존기간이 경과한 후에는 이를 파기하여도 위법이 아니라고 해석을 할 수 있다. 그러나 전

자의무기록(EMR)등은 공간의 제약이 적고, 영구보존이 가능하며, 연구 및 보건의료통계 및 보건정책 연구에도 유용한 자료로 활용 가능하므로 동 규정을 현실화 할 필요가 있고, 개인정보보호법에도 보존의무기간이 경과한 경우 환자의 동의에 의해 보관기간을 연장할 수 있으므로 의무보존 기간을 최소 20년으로 현실화하고 환자의 동의가 있을 경우 연장이 가능한 것으로 개정하는 것이 타당하다고 판단된다.

4. 입법적 보완과 개인정보보호

의료기관에서는 수 많은 환자의 의료정보가 생성되고 가공된다. 의료법 제21조 제2항 등에서는 환자 외의 자에게 환자의 의료정보를 공개할 수 있는 사유를 주체, 공개 상대방, 공개대상, 공개방법, 공개절차 등에 대하여 자세하게 규정하고 있다. 2009. 1. 30. 의료법 개정을 통해 환자에 관한 기록의 열람·사본 교부 등에 관한 절차 및 요건 등을 엄격히 하였다. 구 의료법에서는 ‘이 법이나 다른 법령에 따로 규정된 경우’에는 환자 본인 외의 자에게 환자의 의료정보를 공개할 수 있도록 함으로써, 엄격히 보호되어야 할 환자의 진료 관련 정보가 환자 본인의 동의 없이 누출될 가능성이 있었다. 이에 환자에 관한 기록열람이나 사본 교부를 제21조 제2항 각호에 규정된 경우로 엄격히 제한함으로써 환자의 진료정보 보호를 강화하기 위하여 의료법을 개정한 것이다. 그러나 보관중인 의료정보를 공개하려 할 경우에도 반드시 환자에게 알려야 한다. 이는 환자의 진의의 의사표시를 명확히 할 필요가 있기 때문이다[20]. 흔히 보험사 등에서는 환자의 위임장을 첨부하여 의료정보기록을 열람하는 경우가 많으나 의료정보관리자와 보험사 직원과의 친분관계나 계속적인 업무관계로 인한 업무유착 등으로 악용될 경우 의료정보 보호의 문제점은 쉽게 노출될 수 있고 이로 인한 피

해는 의료정보를 제공한 환자에게 돌아가기 때문에 환자에게 반드시 E-mail 및 유선통화를 실시하여야 하고, 직원들의 정기적인 교육과 의료정보 관리 지침 등의 철저한 제도적 보완이 요구된다. 이는 여전히 의료기관들이 의료정보에 대한 인식이 부족하고 의료정보를 취급하는 부서가 정해져 있다하더라도 현실에서는 의료정보팀 외에도 원무과나 의사, 간호사 및 보건공공기관 등을 통하여 의료정보가 유출되는 것이 의료기관의 현실임을 감안할 때 의료정보관련자 외에 환자의 개인정보를 취급하는 모든 기관과 관련 업무종사자들의 의료정보에 대한 윤리의식 강화를 위한 자정노력은 물론이고 이 외에 별도의 의료정보관리 전문가가 병원 내에 의료정보업무를 수행할 수 있도록 의료관계법 등에 관계 규정의 정비도 필요하다. 물론 개인정보보호법 제35조(개인정보의 열람), 제36조(개인정보의 정정 삭제)권한이 있지만 환자는 이러한 권한을 행사하는 경우가 거의 없고 병원에서 적극적으로 환자에게 설명해야 할 의무가 있다. 특히, 개인병원 등의 사적기관의 의료정보는 개인정보보호에 있어 취약하다고 할 수 있고, 여전히 상당수 의원급은 여전히 수기로 작성된 의료정보를 취급하고 있어 의료정보보호에 취약점이 있다. 최근 보건복지부에서 의료기관 개인정보보호 가이드라인(500병상 이상 의료기관 대상)을 제정·공포하여 2010년 3월 15일부터 시행하고 있으나 병원에서도 가이드라인이라는 강제성 없는 규정의 인식, 감독기관의 감사시행 및 처벌규정의 미비, 병원관계자의 인식부족, 500병상 이상만 대상으로 하고 있다는 점 등의 문제점을 노출하고 있어 실효성이 의문시 된다. 따라서 의료법 시행규칙에 가이드라인을 법제화할 필요가 있다.

IV. 결론 및 제언

오늘날 의료계에는 의료기술의 발전, 국민들의

건강에 대한 관심 증가, 생활수준의 향상으로 의료에 대한 높은 기대와 고급화 경향이 나타나고 있다. 또 의학 지식의 대중화와 권리 의식의 향상에 따라 의료이용자들의 역할도 능동적으로 변화하고 있다[21]. 본 논문에서는 전자의무기록(EMR)의 활용과정에서 발생할 수 있는 환자정보에 관한 문제들을 정보의 수집, 저장, 이용, 파기의 단계로 세분화 하여 그 해결책을 모색하였다. 또한 각 단계의 입법적 보완책을 해석론적 방법과 비교법적 방법을 사용하여 분석함을 본 연구에 목적으로 제시하였다. 전자의무기록(EMR)은 환자의 민감한 의료정보를 담고 있어, 정보수집이나 이용 등에 있어서 환자의 정보보호를 위한 엄격한 제도적 장치와 관리가 필요하다. 과학의 발전과 전자의무기록(EMR)의 네트워크시스템의 활용으로 쉽고 빠르게 의료인 등이 이용할 수 있는 유용성을 가져올 수 있지만, 반대로 불법적인 정보유출이나 병원관계자가 환자의 개인정보를 수집할 경우 충분한 설명의무를 이행한 후에 환자가 이에 대해 명확히 이해하고 결정을 내릴 수 있는 정보주체의 동의(Informed Consent)에 의한 정보 수집이 선결되어야 그 효력이 유효하다고 할 수 있다. 또한 현재 의료법에서 진료기록부의 경우 10년을 최소 보존하여야 한다고 규정하고 있으나, 전자의무기록(EMR)을 활용하는 대부분의 의료기관은 영구보존이 가능하고 전자의무기록(EMR) 등은 공간의 제약이 적고, 영구보존이 가능하며, 연구 및 보건의료통계 및 보건정책연구에도 유용한 자료로 활용 가능하다. 또한 개인정보보호법에도 보존의무기간이 경과한 경우 환자의 동의에 의해 보관기간을 연장할 수 있으므로 의무보존 기간을 최소 20년으로 현실화하고 환자의 동의가 있을 경우 연장이 가능한 것으로 개정하는 것이 타당하다고 판단된다. 전자의무기록(EMR)은 네트워크화 되어 있어 사적 비밀보장과 신뢰성을 확보하기 위한 제도적 장치와 보안의 중요성은 환자의 개인정보보호와

활용을 위해서도 의료기관에 의무적으로 개인정보 관리자의 선임 및 규정이 필요하다. 또한 점점 진화되는 병원정보화(HIS: hospital information system)가 급속히 진행되고 있고, 앞에서 언급한 미국의 경우에도 전자건강기록(EHR)단계에서는 환자의 의료정보뿐만 아니라 민간의료 및 국가수준의 건강문제에 대한 모든 사항이 포함될 수 있는 단계로 전자의무기록(EMR)이 진화될 것으로 예상된다. 전자의무기록(EMR)의 발달은 의료관계인 및 의료기관 등에 많은 편리성 및 유용성을 가져다 줄 수 있지만 반대로 의료정보 위협에 더욱 쉽게 노출시킬 수 있는 문제점도 함께 가지고 있기 때문에 의료정보의 안전성 및 신뢰성을 담보할 수 있는 시설 및 장비의 표준화가 시급하다. 또한 도래하는 미래를 대비하여 발생될 수 있는 문제를 인식하고 대비할 수 있는 개별입법 및 법률의 하위법률의 제정을 모색하여야 한다.

REFERENCES

1. S.S. Kim, C.H. Jung, J.W. Huh(2013), The Effects of Perceived Service Convenience on Job Satisfaction, Organizational Trust and Commitment, and Turnover Intention of Healthcare Service Workers, The Korean Journal of Health Service Management, Vol.7(1);36.
2. J.E. Song, S.H. Kim, M.A. Chung(2006), Home Healthcare Service and Information Protection, Korea Institute of Information Security and Cryptology, Vol.16(6);56-63.
3. Y.J. Jeun(2006), The Medical Information and Privacy Protection, Journal of Korean Law Association, Vol.23;525.
4. J.H. Hong(2012), Management of Medical Record, KMS, Vol.6;181-184.
5. Y.J. Jeun(2007), Legal Issues in The Medical

- Information, Chosun University Law, Vol.14(1);126.
6. Constitutional Court of Korea 2009.09.24, 2008.10.30, 2005.07.21.
 7. K.S. Choi, H.C. Kim(2010), Bioethics & Biosafety law of issue, Seoul, Bioethics Policy Research Center, pp.18-19.
 8. S.M. Lee(2008), The Medical Information and Information Protection, Hanyang University Law, Vol.25(1);42.
 9. Y.J. Jeun(2007), Bioethics and Law, Medical-Korea, pp.157-158.
 - 10.Y.Y. Jeong(2012), A Study on Legal Protection, Inspection and Delivery of the Copies of Health & Medical Data, Journal of Korean Association of Medical Law, Vol.13(1);373.
 11. K.W. Jung(2011), Medical Professional's Rights and Duties Manage Medical Information, HanYang University Law, Vol.28(1);36.
 12. B.G. Jeong(2008), Issues on the Patient's Information Protection, Journal of Korean Association of Medical Law, Vol.9(2);357.
 13. K.H. Kim(2006), Introduction of the EMR System into the Hospital Management and Relevant Issue, Journal of Law and Policy, Vol.6(1);107-108.
 14. D.H. Hyun(2006), A Study of the Improvement of Legal System Involving Health Care Information, Korea Legislation Research, Vol.11;51.
 15. Y.C. Back(2008), America of Privacy Protection and HIPPA, Journal of America constitution Law Association, Vol.19(1);85-94.
 16. H.J. Lee(2012), Problems and Solutions of Personal Information Protection in the Medical Area, Korean Journal of Medicine and Law, Vol.20(2);281-289.
 17. I.Y. Lee(2011), An Analysis of the Major Issues Electronic Medical Records, Hanyang University Law, Vol.28(1);95.
 18. J.S. Getter(2002), Coding for Change: The Power of the Human Genome to Transfer the American Health Insurance System, 28 American Journal of Law & Medicine, p.50.
 19. Y.J. Jeun(2012), The Medical Information Protection and major Issues, Journal of Korean Computer Information Association, Vol.17(10);257.
 20. S.D. Warren, L.D. Brandeis(1890), The Right to Privacy, Harvard Law Review, Vol.4;193.
 21. H.J. Lee, T.Y. Hwang, S.R. Park(2013), Factors for Choice on Dental Care Facilities among Dental Patients in Dageu, The Korean Journal of Health Service Management, Vol.7(1);146.

접수일자 2013년 8월 10일

심사일자 2013년 8월 13일

게재확정일자 2013년 9월 12일