u-Health IT 서비스 환경에서의 개인의료정보보호 수준제고 방안

김동수*°, 김민수**

*숭실대학교 산업·정보시스템공학과, **부경대학교 시스템경영공학과

Issues on Privacy and Security of Health Information in u-Health IT Service Environment

Kim, Dongsoo, Kim, **Minsoo**

Soongsil University, Pukyong National University

E-mail : dskim@ssu.ac.kr, minsky@pknu.ac.kr

요 약

의료기관의 정보화 수준이 높아짐에 따라 권한 없는 자의 정보 접근 및 유출, 진료정보 및 개인정보의 손실이나 파손, 환자 안전에 대한 위협 등 여러 가지 정보보호 리스크 요인이 대두되고 있다. 의료기관이 취급하고 있는 의료정보는 환자 개인을 식별할 수 있는 개인정보뿐만 아니라 개인의 사생활보호 차원에서 신중하게 취급해야 하는 매우 민감한 진료정보를 포함하고 있으므로 정보보호의 중요성이 매우 크다고 볼 수 있다. 따라서 개인의료정보를 컴퓨터와 네트워크를 통해 처리하는 의료기관의 정보보호 수준 제고가 매우 중요하고 시급한 과제로 인식되고 있다. 본 연구에서는 의료기관 정보화의 진전과 원격의료/재택의료의 발전, 국가보건의료정보 인프라 구축, e-Health 및 유비쿼터스 건강관리 시대의 도래 등과 같은 중대한 의료정보 패러다임의 변화 속에서 정보보호의 이슈와 해결방안을 모색해 보았으며, 의료정보보호 수준제고를 위한 정책방향을 제시하였다. 개별 의료기관뿐만 아니라 국가 차원의 의료정보 인프라 구축 사업 추진 시에도 본 연구에서 제안한 의료정보보호 수준제고 방안이 적용되어 정보화의 효율성과 정보보호가 균형을 이룰 수 있을 것으로 기대된다.

1. 서론

오늘날 많은 의료기관이 컴퓨터를 이용하여 정보를 저장, 관리, 이용하여 업무를 수행하고 있다. 보험청구 등과 같은 행정 관리 업무에 주로 사용되던 컴퓨터가 이제는 진료 분야와 경영관리 분야 전반에 걸쳐 그 적용이 확대되고 있다. 임상 진료 분야의 정보 시스템뿐만 아니라 ERP, CRM, SCM 등 경영관리 및 외부기관과의 협력 및 통합 시스템에 이르기까지 정보시스템 의존도가 커지고 있다. 특히, 환자 진료정보의 핵심적 내용을 포함하고 있는 전자의무기록 시스템 도입이 가속화 되면서 컴퓨터와 네트워크를 통한 정보의 원활한 접근, 관리, 공유가 이루어지지 않고서는 의료기관의 업무가 효율적으로 진행되기 어려운 상황이다.

병원의 운영 업무와 진료 업무가 정보시스템에 의존하는 비중이 높아짐에 따라 정보보안 위협은 더욱 커지고 있다. 의료정보화가 발전되고, 국가 차원의 보건의료정보인프라 구축 논의가 진전되어 감에 따라 환자의 개인정보와 의료정보의 보호가 매우 중요한 이슈로 부각되고 있다. 인터넷을 통한 의료기관 간 의료정보의 공유가 의료 협력 네트워크상에서 진행되고 있고, 전자의무기록이 개별 의

료기관 내에 존재하는 것이 아니라 개인의 평생 전자건강기록 차원에서 사용될 것으로 전망되고 있다. 아울러 원격의료 및 재택의료의 확산과 유비쿼터스 기술의 의료 분야 보급으로 u-Health의 등장 등 의료 환경이 병원 내에서 벗어나 환자의 집이나 이동 공간을 포함한 생활공간으로 확대됨에 따라 새로운 보안 요구가 생겨나고 있다.

의료정보화의 진전으로 인해 권한 없는 자의 정보 접근 및 유출, 진료정보 및 개인정보의 손실이나 파손, 진료정보의 일시적 손실이나 접근불가, 환자 안전에 대한 위협 등 막중한 정보보호 리스크가 생겨나고 있다. 특히 의료정보는 환자 개인을 식별할 수 있는 개인정보와 개인의 사생활보호 차원에서 매우 신중하게 취급해야 하는 민감한 진료정보 등을 포함하고 있으므로 의료기관의 정보보호 수준 제고를 위한 국가 차원의 노력이 요구된다 할 수 있다.

국내 의료기관에서 환자정보를 보호하기 위한 체계는 아직 미진한 것이 사실이다. 일부 대형 병원을 제외하고는 아직 네트워크와 PC 레벨의 보안 투자를 진행하고 있는 수준이기 때문이다. 전자의무기록, OCS 등의 정보시스템에 대한 사용자 인증과 접근제어 및 권한관리, 의료정보에 대한 전자서명 및 암호화, 감사 및 추적체계 등 시스템 차원의 보안 대책과 보안정책 및 관리적 차원의 보안 관리 체계가 정비되지 못한 의료기관이 매우 많은 실정이다.

본 연구에서는 의료기관 정보화의 진전과 원격의료/재택의료의 발전, 국가보건의료정보 인프라 구축, e-Health 및 유비쿼터스 건강관리 시대의 도래 등과 같은 중대한 의료정보 패러다임의 변화 속에서 정보보호의 이슈와 해결방안을 모색해 보았으며, 의료정보보호 수준제고를 위한 정책방향을 제시하였다. 개별 의료기관뿐만 아니라 국가 차원의 의료정보 인프라 구축 사업 추진 시에도 본 연구에서 제안한 의료정보보호 수준제고 방안이 적용되어 정보화의 효율성과 정보보호가 균형을 이룰 수 있을 것으로 기대된다.

2. 의료정보보호의 개념

2.1. 정보보호의 개념

정보보호는 조직의 손실을 최소화하고 이익을 최대화하기 위하여 다양한 위협으로부터 정보를 보호하는 것을 말한다. 정보보호의 3요소로 비밀성, 무결성, 가용성을 유지하고 보장해야 한다. 비밀성(confidentiality)이란 데이터나 소프트웨어에 대한 불법적인 접근에 관한 문제로써 접근이 인가된 사람에 한해 정보에 접근할 수 있도록 보장하는 것이다. 무결성(integrity)은 비밀성과 밀접한 관계를 가지고 있다. 불법적이거나 고의적인 사고에 의해 데이터가 변경되거나 삭제되지 않도록 하는 것으로 정보와 정보처리 방식의 정확성과 완전성을 보장하는 것을 말한다. 가용성(availability)은 인가된 사람이 원할 때에 정보통신 시스템이 적절한 방식으로 작동하는 것을 의미하므로 인가된 사용자가 필요할 때에는 정보 및 이에 관련된 자산에 접근할 수 있는 것을 보장하는 것이다.

2.2. 개인정보보호

개인정보란 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등의 사항에 의하여 개인을 식별할 수 있는 정보를 말하며 그 정보만으로 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 정보를 포함한다. 개인정보는 본인의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 정보주체(혹은 당사자)의 안녕과 이해관계에 영향을 미칠 수 있는 개인과 관련된 모든 정보로 폭넓게 해석할 수 있다[6].

당해 정보주체와 관련된 제반의 정보가 오남용(도용, 변경, 유출, 훼손 등)됨으로써 정보 주체의 자기정보통제권이 침해되는 것을 개인정보의 침해라 한다. 개인정보는 인격을 이루는 요소이면서 표현의 자유 등 헌법상 인정되는 다양한 기본권과 밀접한 관련이 있는 정보로서 오남용될 경우 개인의 인격적, 재산적 권익을 손상시킬 우려가 있으므로 모든 개인정보는 개인의 인격 존중 이념에 따라 신중히 취급되어야 한다[1].

급속한 정보기술의 발전으로 인해 특정인에 대한 개인정보의 수집, 관리, 이용 등의 정보 활용이 보다 용이해 졌다. 특히, 우리나라에서는 전 국민을 대상으로 주민등록번호라는 개인 식별번호를 개인 식별자 및 개인정보의 통합을 위해 사용하고 있다. 따라서 정보통신망에서 개인정보의 연결이나

교차참조가 쉽게 이루어질 수 있으며 정보의 중앙 집중화를 초래하여 개인정보의 유출 및 오/남용의 가능성을 증가시켜 잠재적 프라이버시 위협이 매우 크다고 볼 수 있다[6]. 또한 컴퓨터에 저장되어 있는 개인정보는 컴퓨터 바이러스 및 악의적인 해커에 의한 시스템 파괴 및 정보유출 등의 잠재적 위험요소를 안고 있다.

2.3. 의료정보의 개념 및 정보보호의 중요성

의료정보라 함은 의사가 환자에 대한 의료행위를 하면서 수집된 자료들과 이 자료들을 기초로 연구 분석된 정보들을 포함하는 것으로써 진단과 그에 따른 치료행위 및 치료경과에 따른 면밀한 관찰 등을 모두 포함하는 전체과정에서 수집된 자료들을 의미한다[5]. 즉, 개인의 신체적, 정신적 상태나 기능적 상태에 관한 예방, 진단, 치료 및 재활과 관련된 의무기록, 연구결과 정보, 의학정보 및 원무정보를 말한다. 이는 개인의 가족 사항, 유전적 특징, 병력, 약물 중독 내용, 성병 등에서부터 개인의 신분, 재산, 가족, 사회생활, 성생활, 습관에 이르기까지 매우 민감한 정보를 포함하고 있다.

이러한 보건의료정보는 의료인이 환자를 진료함에 있어서 중추적인 역할을 하며, 국가적 차원의 보건 정책을 위한 자료 제공의 역할에서부터 각종 보건 의료 종사자들에 대한 정보 제공과 각 분야의 실무 종사자가 필요로 하는 정보제공의 역할까지 담당한다.

의료정보는 병원의 내/외부적으로 다양하게 사용된다. 환자 진료 및 치료, 처방에 사용되는 것을 비롯하여 연구를 목적으로 한 조사, 법률적 자료(소송에 따른 증거), 의료비 청구 등에 사용된다.

의료정보는 개인의 프라이버시를 포함한 민감한 정보임에도 불구하고, 다양한 사람들로부터 정보의 공개 및 사용이 요구된다. 이러한 의료정보는 특히 의료기관의 정보화가 가속화되고 인터넷을 통한 정보 접근가능성이 확대되면서 의료정보의 손실이나 파손으로 인한 환자 안전에 대한 위협, 환자 진료정보나 개인정보에 대한 권한이 없는 자의 접근이나 정보유출로 인한 비밀성 침해, 필요한 정보서비스 제공의 불가 등 여러 가지 정보보호 리스크를 안고 있다. 환자 개인의 프라이버시에 대한 침해뿐만 아니라 정보의 무결성을 침해하여 부정확한 정보의 제공으로 환자 진료 시 막중한 위험을 초래할 수도 있다. 또한 정보보호 사고가 발생하게 되면 의료기관 등의 조직 평판 및 대중적 신뢰도 하락 등의 위험이 발생한다. 이러한 위험으로부터 환자의 의료정보를 보호하기 위해서는 의료기관 직원에 대한 보안 교육 실시와 마인드 제고가 필요하다.

환자의 개인의료정보를 보호하고 프라이버시 침해를 방지하기 위해서는 의료정보를 취급하는 의료기관을 포함한 모든 관련 기관의 정보보호 수준 제고가 필요하다. 국가보건의료정보 인프라와 전자건강기록(EHR: Electronic Health Record) 시스템의 정착, 원격의료, 유비쿼터스 건강관리 등 가까운 미래에 도래하게 될 새로운 보건의료정보 인프라 및 서비스의 안전한 정착을 위해서는 의료정보에 대한 프라이버시 리스크를 줄이고 의료기관의 정보보호 수준을 제고하기 위한 국가차원의 관심과 노력이 필요하다.

의료기관 입장에서도 IT 투자시 정보보호를 동시에 고려하여야 하며, 보안 시스템 구축 이전에 정보보호 규정과 조직, 보안 관리 체계 등이 우선 확보되어야 한다. 새로운 취약점은 지속적으로 발생하며, 새로운 시스템 도입은 반드시 새로운 취약점을 유발하므로 시스템 개발 단계에서 보안요소의 검토가 필수적이다.

3. 개인의료정보보호 관련 법제도 현황

현행 의료관련 법령들은 환자의 보건의료정보 보호에 관한 여러 가지 규정을 두고 있다. 보건의료기본법이나 의료법에서 의료정보보호에 관한 조항을 포함하고 있다. 그 외에도 약사법, 전염병예방법, 장기등이식에관한법률, 정신보건법, 생명윤리및안전에관한법률, 후천성면역결핍증예방법 등에서 환자의 의료정보에 관한 '비밀누설의 금지'와 관련한 조항을 두고 있다.

보건의료기본법은 보건의료서비스에 관한 국민의 자기결정권을 규정하고, 보건의료에 관한 국민의 알권리와 비밀보장, 보건의료에 관한 국민의 의무 등 보건의료정보에 대한 국민의 권리와 의무를 전체적으로 포괄하여 규정하고 있다.

의료법에서는 비밀누설의 금지, 기록 열람과 관련한 규정을 포함하고 있다. 2003년 9월 개정된 의

료법에는 전자처방전, 전자의무기록 관련 조항 등이 새로이 신설되었다.

그 외 약사법, 전염병예방법, 장기등이식에관한법률, 정신보건법, 생명윤리및안전에관한법률, 후천성면역결핍증예방법 등의 개별 법령에서 환자의 개인의료정보 보호를 위한 규정을 포함하고 있다.

의료정보보호에 관한 조항이 개별 법령에 산재되어 있고 기본적인 원칙과 종합적인 보호 규정이 미비하다는 지적에 따라 현재 보건복지부에서는 보건의료정보화촉진및의료정보보호에관한법률(가칭)안을 마련 중이다. 이 법률 제정 작업의 모태가 되는 [5]에서는 다음의 규정을 포함하고 있다.

① 개인보건의료정보의 수집, 처리, 이용 및 제공 등: 동의에 의한 수집, 수집 시 고지의무, 개인보건의료정보 수집의 제한, 개인보건의료정보의 처리, 이용 및 제공, 연구목적에 의한 개인보건의료정보의 처리, 이용 및 제공, 개인보건의료정보의 파기
② 정보주체의 권리: 자기결정권, 개인보건의료정보에 대한 접근 권리, 개인보건의료정보에 대한 수정 요청의 권리, 제3자 제공 내역서를 받을 권리, 제한 요청의 권리, 비밀 의사소통 요청의 권리, 동의철회의 권리
③ 보건의료정보취급자의 의무: 보건의료정보취급자의 책임, 개인보건의료정보관리책임자의 지정, 개인보건의료정보의 보호조치, 비밀유지, 요청 및 불만의 처리

4. u-Health의 진전과 정보보호

4.1. 전자의무기록과 정보보호

환자의 진료 과정에서 생성되는 정보를 컴퓨터를 이용하여 입력, 저장, 관리하는 전자의무기록 시스템은 종이기반 의무기록에 비해 접근성이 뛰어나고 정보 공유가 가능하다는 점, 의사결정 지원 기능 등을 포함한 진료의 질 향상 등 여러 가지 장점으로 인해 국내외 의료기관에서 많은 관심을 갖고 있다. 그런데, 전자의무기록에는 환자의 진료정보 뿐만 아니라 환자 개개인을 식별할 수 있는 개인정보를 포함하고 있기 때문에 보안이 매우 중요하다.

2005년 2월에 발표된 전자의무기록의 프라이버시 리스크에 대한 조사 결과에 의하면 미국 성인의 70%가 데이터 보안 상 문제점으로 인해 개인의 보건의료정보가 유출될 수 있다고 우려하고 있다[7]. 동 조사에서 응답자의 69%는 전자의무기록 시스템을 통해 환자가 인지하지 못한 상황에서 건강정보 공유가 더 많아질 것을 우려하고 있으며, 47%는 전자의무기록의 장점보다 프라이버시 리스크가 더 크다고 생각하는 것으로 조사되었다.

전자의무기록을 도입하게 되면 진료정보가 컴퓨터를 통해 처리되므로 권한 없는 사람의 임의적 접근 및 정보 유출, 정보의 위변조, 해킹을 통한 시스템 파괴 등 보안 리스크가 존재한다. 따라서 전자의무기록 시스템을 도입하는 의료기관에서는 이러한 리스크에 대응할 수 있는 보안 체계를 갖추어야 하며, 침입차단시스템(firewall), 암호화, 접근권한 관리 등과 같은 기술적인 대책뿐만 아니라 보안 정책을 포함한 관리적 보안 대책, 물리적 보안 대책 등을 종합적으로 마련해야 한다.

현행 의료법에서는 전자의무기록을 전자서명법에 의한 전자서명이 기재된 문서로 정의하고 있다. 전자의무기록의 안전성을 위해 필요한 시설 및 장비에 대한 기준을 포함하고 있고, 정당한 사유 없이 개인정보를 탐지하거나 누출·변조 또는 훼손해서는 안 된다는 규정이 포함되어 있다. PKI(Public Key Infrastructure) 전자서명이 매우 우수한 보안 기술이며 많은 보안 요구사항을 충족시켜 주는 것은 사실이지만 전자서명만으로 보안과 관련한 문제가 모두 해결될 수는 없다. 따라서 전자의무기록의 생성, 보관, 열람, 유통, 폐기 등 전 수명주기에 걸쳐 각 단계마다 취해야 할 보안 표준 또는 지침이 구체적으로 마련되어야 한다.

전자의무기록이 의료기관 경계를 넘어서서 진정한 개인의 평생 건강기록인 EHR 개념으로 발전하기 위해서는 전자의무기록에 대한 정보보호 수준 제고와 함께 개인의료정보 보호 마인드 제고가 필요하다. 환자 진료를 위한 정보의 공유 및 사용과 정보보호 및 프라이버시 보장이 균형화될 때 보안에 대한 우려가 해소될 수 있다.

4.2. 유비쿼터스 의료 환경에서의 정보보호

정보통신 기술을 활용하여 물리적으로 떨어져

있는 환자에 대해 의료서비스를 제공하거나 지원하는 원격의료 개념은 최근 들어 생체계측 기술과 유비쿼터스 센서, 네트워크 등 관련 기술의 발전으로 유비쿼터스 환경에서의 질병관리 및 건강관리라는 개념으로 발전하고 있다.

유비쿼터스 컴퓨팅의 활용 분야 가운데 가장 기대효과가 클 것으로 주목받고 있는 분야 가운데 하나가 유비쿼터스 건강관리(u-Health) 분야이다. 원격의료의 발전된 형태로 관심을 끌고 있는 유비쿼터스 건강관리는 당뇨, 고혈압과 같은 만성질환자의 관리, 심장질환자의 건강관리, 산모와 태아의 건강관리, 노인 및 장애인의 건강관리 등 다양한 분야에 걸쳐 서비스가 개발되고 있다.

u-Health에서는 환자의 생활공간에서 여러 가지 생체 정보를 수집해 내기 위해 다양한 스마트 센서들의 네트워크가 필수적이다. 스마트 센서들은 환자의 의료정보를 수집하고, 집안 곳곳에 설치된 비디오 센서들은 환자의 움직임을 관찰하여 환자의 상태를 체크한다. 이들 센서들이 산출한 정보는 개인 의료 상담 시스템에 전달되고, 의료 상담 시스템에 기록된 데이터는 병원의 의사나 간호사 등에 전송되어 환자에서 피드백을 하게 된다.

많은 의료기관들이 RFID(Radio Frequency Identification)를 이용한 환자의 식별, 자산의 관리, 약물 투약 추적 시스템 등의 도입과 같은 유비쿼터스 병원(u-Hospital)에 대해 주목하고 있다. 흔히 전자태그라고 불리는 RFID가 확산되고 있는데, RFID는 바코드를 대체할 수 있는 기술로 주목받고 있지만 과다한 개인정보의 수집과 이용 논란을 유발할 수 있다. 그 외 LBS(Location Based Service), 스마트카드 등 새로운 기술의 등장으로 인해 개인정보의 수집, 전송, 통합이 더욱 용이해지고 있다.

유비쿼터스 환경에서 제대로 된 서비스를 제공하기 위해서는 유비쿼터스 상황(Context) 인지가 필요하므로 개인이 자신의 정보를 일정부분 공개하는 것이 필수적이라 할 수 있다. 첨단 정보기술 및 유비쿼터스 인프라를 통해 고품질 개인맞춤형 서비스를 제공받기 위해서는 개인정보의 공개를 감수해야 하고 이는 개인정보 유출로 인한 피해 가능성이 높아진다는 것을 의미한다. 따라서 유비쿼터스 건강관리 시스템을 설계할 때에도 정보보호 문제가 설계 단계에서 고려되어 적용되지 않는다면 새로운 취약점과 유출 사고가 자주 발생할 것이다.

시민단체나 전문가들은 유비쿼터스 컴퓨팅 기술이 확산될 경우 새롭게 발생할 역기능에 대해 경고하고 있다. 녹색소비자연대에서는 인터넷실명제, RFID 내 개인정보 수집 허용 등으로 '유비쿼터스 감시사회 도래를 우려'한다는 성명을 2005년 7월 발표한 바 있다.

유비쿼터스 사회로의 이행에 있어 주요 장애 요인인 정보보호 우려를 해소하기 위해서는 컴퓨팅 환경의 변화에 맞춰 현재의 법제도를 보완하고 기술을 지속적으로 연구해야 한다[2]. 유비쿼터스 환경에서는 개인정보 수집이 더욱 용이해지고 이를 분석, 활용하고자 하는 기업 혹은 기관의 욕구가 커질 것으로 예상되므로 개인정보의 수집뿐만 아니라 이를 분석하고 처리하는 과정에 대한 명확하고 세밀한 규정이 필요하다. ID 도용이나 도청, 정보 왜곡 등 위협요인을 제거하기 위한 인증기술, 암호화, 전자서명 기술 등이 활용될 수 있다.

4.3. 국가의료정보인프라 구축과 정보보호

의료소비자의 진료정보가 개별 의료기관 내에서만 접근 가능한 것이 아니라 통합된 정보이자 개인의 평생 건강기록이라는 개념을 근간으로 하는 국가 정보 인프라 구축을 위한 노력이 미국 등 선진국가에서 <표 1>에서 보는 것처럼 활발히 진행되고 있다[3].

<표 1> 주요국의 국가 보건의료정보화 사업

구분	미국	영국	호주	캐나다
프로그램 명칭	NHII[1]	NPfIT[2]	Health Connect	Health Infoway
연결모형	분산형	중앙집중형	중앙집중형	분산형
DB 소재	국가 (인덱스 DB)	지역 및 국가	지역 및 국가	지역 및 국가
접근가능 데이터	환자의무기록 전체	환자의무기록 전체	환자기록요약	환자의무기록 전체 및 요약
접근권한	기관/개인	기관/개인	기관/개인	기관/개인

국내에서도 '언제 어디서나 안전하게 접근할 수

1) National Health Information Infrastructure
2) National Programme for IT

있는 전국민 전자건강기록 시스템을 구축하여 질 높은 의료서비스의 편리하고 효율적인 보장'을 목표로 전자건강기록 체계 구축, 보건의료정보표준화, 개인의료정보보호 등 여러 가지 노력이 진행되고 있다.

이러한 노력을 통칭해서 국가보건의료정보인프라(NHII: National Health Information Infrastructure)라고 지칭하고 있는데 이러한 보건의료정보 인프라는 방대한 정보의 수집 및 저장, 인터넷을 통한 정보 전송 및 공유를 전제로 하고 있어 보안 및 프라이버시에 대한 우려가 크다. <표 2>는 세 가지 NHII 아키텍처 유형과 각 유형별 정보보호 측면에서의 장단점을 보여 주고 있다.

<표 2> NHII 아키텍처 대안 비교

아키텍처 유형	정보보호 측면의 장점	정보보호 측면의 단점
영국식: Centralized EHR 중심의 정보 통합 체계	- 집중으로 인한 효율적 관리	- 정보의 집중으로 인해 프라이버시 우려가 매우 큼(Big Brother, 전자정보통제 우려) - 의료기관 입장에서도 중앙통제에 따른 의료정보 유출 우려 존재 - 통합운영센터의 정보보호 수준을 높이기 위한 고도의 기술, 운영 관리 체계 필요
미국식: Decentralized 아키텍처	- 프라이버시 침해 우려가 상대적으로 적음	- 의료기관이 정보보호 및 보안관리 책임을 짐 - 의료기관의 정보보호 수준을 높이기 위한 표준 및 지침이 매우 중요
혼합식: 공공의료부문은 집중형, 민간의료부문은 분산형 아키텍처	- 비교적 통합이 용이한 공공의료 부분만 통합함으로써 프라이버시에 대한 우려는 최소화하고 효율적 관리 체계를 확보할 수 있음	- 시스템 아키텍처가 복잡하고, 분산형, 집중형에서 발생할 수 있는 문제점을 모두 포함하고 있음 - 민간 영역과 공공 부문의 정보 통합 이슈가 존재

국가적 보건의료정보 인프라가 원활히 구축되기 위해서는 국민의 프라이버시 보장을 위한 법제도 정비와 의료기관의 정보보호 수준제고가 선결과제라 할 수 있다. 날로 발전하고 있는 정보화 수준에 비해 환자 혹은 국민의 프라이버시 보장과 의료정보보호에 대한 인식 수준이 상대적으로 낮은 국내 현실을 감안할 때 우선적으로 국민 개개인의 프라이버시 보호를 위한 기본 원칙과 종합적인 규정이 마련되어야 한다. 유무선 네트워크상의 정보 도청 등과 같은 기밀성 침해, 데이터의 임의적인 위·변조 및 손상과 같은 무결성 침해 및 시스템 가용성 침해 요인으로부터 보건의료정보를 보호하기 위한 종합적인 정보보호 체계 또한 마련되어야 할 것이다.

5. 의료정보보호 정책방향

앞서 살펴본 바와 같이 전자의무기록의 도입 및 발전, 유비쿼터스 건강관리, 국가보건의료정보인프라 구축 등 e-Health가 발전하면서 의료정보의 보호가 더욱 중요해지고 있고 정보보호 리스크에 대한 우려도 커지고 있다. 따라서 개인정보보호를 위한 국가 차원의 노력과 함께 의료기관을 포함한 의료정보 취급기관의 정보보호 수준제고를 위한 체계적이고 종합적인 노력이 필요하다.

개인의료정보보호를 위한 법제도 개선을 통해 국민 개개인의 프라이버시를 최대한 보장해 줄 수 있어야 하고, 의료정보 보안 표준안을 마련하여 보급함으로써 개별 의료기관의 정보보호 수준을 제고해야 한다. 개별 의료기관들도 정보보호 아키텍처를 정비하고 신규 도입 시스템에 대한 보안성을 강화하는 등 정보보호를 위한 노력을 기울여야 한다. 또한 보건의료인의 정보보호 인식 수준을 높이고 정보보호의 중요성을 알리기 위한 윤리 강령의 제정 및 보급과 함께 정보보호 관련 교육도 필요하다. 국가보건의료정보인프라와 같이 정보공유를 필수요소로 하는 체계 구축을 위해서는 프라이버시 보장과 개인의료정보보호를 최대한 고려해야 한다.

의료정보보호를 위한 핵심 정책방향이라 할 수 있는 프라이버시 보호를 위한 법제도 정비와 보안표준안 개발 방향에 대해서 다음에 상세히 서술하고 의료기관의 대응방향에 대해서 논하였다.

5.1. 프라이버시 보호를 위한 법제도 정비

환자 의료정보에 대한 접근 권한과 공개에 대한 조건을 정함으로써 환자 개인 보건의료정보에 대한 프라이버시를 보장할 수 있다. 국내에서도 미국의 HIPAA 프라이버시 규정과 기타 국내외 관련 법령 등을 참조하여 환자의 개인의료정보 보호를 위한 법 제정 작업이 진행 중이다.

의료계, 시민단체, 정보보호 전문가 등의 의견을 수렴하여 법률 제정을 추진 중인데, 이 법안에는 개인의료정보의 수집, 처리, 이용 및 제공과 관련한 기준과 자기결정권, 접근권리, 수정 요청 권리 등 정보주체의 권리를 보장하기 위한 조항, 보건의료정보취급자의 의무에 관한 규정 등 의료정보보호의 기본원칙 및 규정이 포함될 것으로 전망된다.

국내 의료 환경과 프라이버시에 대한 인식 수준 등을 고려하여 의료 현장에서 현실적으로 수용 가능한 법률의 제정이 이루어져야 할 것이다. 또한 정보보호 측면을 지나치게 강조하여 진료 목적의 정보의 공유나 사용이 지나치게 제한되는 방식으로 추진되어서는 곤란할 것이다. 정보화의 효율성과 개인의료정보의 보호가 균형이 될 수 있도록 프라이버시 규정이 제정되는 것이 바람직하다. 또, 의료서비스 제공자는 정보보호의 중요성을 인식하고 정보화의 역기능 가운데 하나인 보안 리스크를 해소하기 위한 내부적 노력을 기울여야 한다.

5.2. 보안(Security) 표준안의 개발 및 보급

정보보호의 3대 요소인 비밀성, 무결성, 가용성을 보장하기 위한 보안 대책을 표준 규정으로 개발하여 보급하여 개별 의료기관의 정보보호 수준을 제고할 필요가 있다. 현재 국내에는 보건복지부 보건의료정보표준화 위원회 산하에 정보보호 분과 위원회가 설치·운영 중인데 정보보호 분과에서 보안 규정을 제정하기 위한 노력을 진행 중이다. 보안관리 프로세스, 보안 책임자 지정, 인력 보안관리 및 교육, 정보접근 관리 정책 등과 같은 관리적 대책과 의료기관의 정보시스템 및 관련 건물, 장비들을 자연 재해나 환경적 위험요인, 불법적인 침입으로부터 보호하기 위한 물리적인 수단, 정책, 절차를 의미하는 물리적 대책, 전자화된 건강 정보의 보호와 접근 제어에 사용되는 기술, 정책, 절차를 의미한 기술적 대책이 보안 표준의 주요 내용이 된다.

보안 표준의 규정에 구체적 기술을 명시하는 방식 보다는 보안 요구사항을 해결하기 위한 포괄적이고 중립적인 정책, 절차, 기술을 주 내용으로 하는 것이 바람직하다. 정보보호 분과에서는 HIPAA의 보안 규정[8] 등 국외 관련 규정 및 표준안을 참조하고, 국내의 전자의무기록 보안 표준화 연구 결과로 제시된 보안 인증 평가항목을 활용하여 종합적이고 구체적인 보안 표준의 제정을 추진하고 있다.

의료기관이 세부 보안 규정에서 정의하고 있는 사항을 충족시키기 위해서는 추가적인 비용과 노력이 필요하다. 이러한 비용과 노력은 정보화를 통한 효율성 제고와 환자 개인의료정보의 보호라는 두 가지 목표를 충족시키기 위해 지불해야 하는 비용이라 할 수 있다.

일단 표준이 제정되어 보급되고 나면 의료기관이 보안 표준을 얼마나 준수하는지 평가하고 인증하기 위한 체계가 필요하다. 보안 표준에 대한 인증 체계는 국외 사례와 국내 타 분야의 사례를 참조하여 최적의 방안을 모색할 필요가 있다. 보안 표준의 준수가 의료기관의 일방적인 부담으로만 작용해서는 곤란하며, 의료기관이 개인정보보호 규정 및 보안 표준을 잘 따르면서 효율적인 정보 이용과 정보보호를 동시에 달성할 수 있도록 제반 여건을 조성해야 한다.

5.3. 의료기관의 대응방향

국내 의료기관들은 정보보호의 걸음마 단계라 할 수 있는 네트워크 보안, PC 레벨의 보안 및 단편적 보안 솔루션 도입에 머무르고 있다. 이러한 초보적인 수준에서 탈피하여 보안 관리 체계를 정립하고 종합적인 정보보호 마스터 플랜에 입각한 정보보호 프로세스 확보 및 정보보호 문화의 달성이라는 보다 향상된 정보보호 수준으로 나아갈 필요가 있다.

이를 위해 의료기관을 포함하여 모든 의료정보 취급기관들은 전사적 정보보호 아키텍처를 갖출 필요가 있다. 정보보호 정책 및 정보보호 관리 절차 및 규정, 조직 체계를 확보하고 정보보호 아키텍처 전반에 걸쳐 체계성을 확보하여 정보보호 기반을 마련해야 한다. 조직의 모든 구성원들이 정보보호에 대한 인식을 전환할 수 있도록 교육과 훈련을 실시하는 등 정보보호 문화의 확산을 위한 노력이 필요하다.

의료기관들은 프라이버시 규정이나 보안 표준과 같이 의료정보보호와 관련한 국가 차원의 법제도를 준수할 수 있도록 대비해야 한다. 현재 국가 차원에서의 개인정보보호법이나 의료정보보호 관련

규정의 제정 작업이 진행 중이므로 전자의무기록 등 의료정보화 시스템을 구축하는데 있어 정보보호를 보다 강화할 필요가 있다. 각 의료기관별로 환자의 개인의료정보보호 수준진단 및 보호 대책을 마련하고 시급한 대책부터 우선적으로 실시해야 할 것이다.

정보보호는 일시적인 노력으로 해결되는 것은 아니다. 신규 자산 및 정보시스템의 확충, 새로운 위협 및 취약성의 증가 등으로 인해 새로운 보안 위험은 나타나기 마련이다. 따라서 지속적인 정보보호 관리 체계를 갖출 필요가 있다. 특히, 최근 나타나고 있는 웹기반 의료정보시스템, 웹 서비스 방식의 의료정보 시스템 통합 등과 같은 새로운 서비스 제공방식에서 발생 가능한 보안 위험을 해소하기 위해서는 시스템의 분석 및 설계 단계에서부터 정보보호를 고려하여 새로이 제공되는 서비스의 보안성을 확보할 필요가 있다.

6. 결론

본 논문에서는 의료정보보호와 관련한 기본 개념을 소개하고, 국내외 법제도 현황을 요약 제시하였다. 또한, EHR 개념으로의 발전, 원격의료 및 u-Health의 도래, 국가보건의료정보인프라 구축 논의 등 e-Health의 진전에 따른 정보보호 이슈를 살펴보고, 의료정보보호 수준제고를 위한 정책방향을 제시하였다.

의료기관의 정보보호 수준을 높이기 위해서는 국가 차원에서 제정한 보안 기준에 의거 병원 자체의 내부 보안정책과 규정, 그에 따른 감시 및 감사 체계가 마련되어 있어야 하며, 정보보호 기술 및 장비에 대한 투자와 이를 운영하는 전담 조직이나 인력이 필요하다. 비용과 관리 인력의 증가, 사용상의 불편 등을 초래한다는 이유로 더 이상 보안을 늦출 수는 없다.

의료기관 간 정보공유와 협진체계 마련, 인터넷을 통한 환자 진료정보의 제공 및 의사소통, EHR을 통한 평생 건강 기록의 구축 등이 가시화되고, e-Health를 넘어 유비쿼터스 기술을 활용한 건강관리 시대로 접어들 것이 예상되고 있는 만큼 본 연구에서 제안한 환자 프라이버시 보호를 위한 규정의 제정과 보안 관리체계와 정책, 전담 인력의 확보, 기술적 보안 대책의 수립 등의 보안 규정의 수립은 반드시 추진되어야 할 것이다. 개별 의료기관들도 정보화 추진에 있어 환자의 개인의료정보의 보호와 보안 수준의 확보를 중요하게 고려해야 한다.

최근 병원들이 전자의무기록을 핵심으로 하는 병원정보화 추진과 함께 보안에 대한 중요성을 인식하고 관련 분야에 대한 투자와 노력을 기울이고 있는 것은 매우 다행스러운 일이다[4].

그럼에도 불구하고 환자정보를 보호하기 위한 체계는 아직 미진한 것이 사실이므로 병원정보화 및 e-Health의 진전에 따른 정보보호의 중요성을 인식하고 기술적 보안 대책뿐만 아니라 정보보호 정책 수립 등을 포함한 관리적 보호 대책과 물리적 보안 대책을 수립하여 개인의료정보의 보호에 힘써야 할 것이다.

[참고문헌]

[1] 강달천, 「정보통신환경의 변화와 개인정보보호」, 『개인정보보호 정책 포럼』, 한국전산원, 2004.5.

[2] 김태중·김인호, 『유비쿼터스 환경에서의 개인정보 관리체계에 관한 연구』, 정보보호뉴스, 2005.3., pp. 10 ~ 15.

[3] 보건복지부, e-Health 분과협의회 워크샵-국가보건의료정보화 계획(안), 2005.6

[4] 이유지, 『정보보안 투자에 나선 병원, 그 현황과 과제』, 컴퓨터월드, 2005.7

[5] 채영문, 「e-Health 발전을 위한 제도 개선방안 수립」, 보건복지부, 2005.4.

[6] 홍성걸, 「개인정보보호와 정책갈등-NEIS사례를 중심으로」, 『ISR』, 제1권 2호, 한국정보보호진흥원

[7] P&AB and Harris Interactive, http://www.pandab.org/healthpr.html Accessed Sep. 17, 2005

[8] United States Department of Health Human Service, "Standards for Privacy of Individually Identifiable Health Information, Security Stands for the Protected Health Information, General Administrative Requirements Including, Civil Money Penalties", Regulation Test(45 CFR Parts 160 and 164)