情 報 保 護 學 會 誌
第19卷 第1號, 2009. 2

보건의료의 정보화와 정보보호관리 체계

정 혜 정*, 김 남 현**

요 약

윤택하고 건강한 삶에 대한 인간 본연의 욕구와 급격한 정보화 흐름의 시대적 만남은 보건의료정보 교류를 위한 연구 개발을 가속하는 한편, 개인의 가장 민감한 정보인 보건의료정보를 위험으로부터 어떻게 보호할 것인가에 관한 우려 또한 증대시키고 있다. 본 논문에서는 보건의료정보화 현황을 고찰하고 HL7, CCHIT, 그리고 보건복지가족부 등에서 추진 중인 보건의료 분야의 정보보호관리 표준화 동향을 소개하였다.

Ⅰ. 서 론

언제 어디서나 개인의 건강을 증진시키고 만성질환을 관리하며 급성질환을 예측하는 유비쿼터스 건강관리 시스템이 차세대 보건의료정보화의 핵심 동력으로 기대되면서 범국가적 차원의 인프라, 요소기술 개발 등 정보기술에 기반을 둔 연구가 활발히 진행되고 있다. 보건복지부는 2010년까지 원하는 국민 모두가 전자건강기록을 통해 질 높은 의료서비스 이용의 편리성과 효율성을 보장 받을 수 있는 시스템을 제공한다는 목표로 총 1조 800여 억 원의 비용을 투자할 계획임을 밝힌바 있다[1].

더불어 정보화가 진행될수록 정보보호의 중요성 또한 더욱 부각되고 있다. 보건의료기본법[2]에 의하면 보건의료정보란 '국민의 건강을 보호·증진하기 위하여 국가·지방자치단체·보건의료기관 또는 보건의료인 등이 행하는 모든 활동과 관련한 지식 또는 부호·숫자·문자·음성·음향 및 영상 등으로 표현된 모든 종류의 자료'로 일반 개인정보와 차별하여 정보 수집을 제한하고 있는 민감한 정보다. 보건의료정보가 당해 의료기관 내에서 수집·이용되는 것에 그치지 않고 시공간의 제약 없이 수집되어 기관 간, 국가 간에 전자적으로 교환 및 활용되는 환경에서 개인의 자기 정보 통제는 점점 더 어려워지고 있다. 이를 증명이라도 하듯 정보 유출 사고가 나날이 증가하고 있으며 보건의료 분야도 예외가 아니어서 정보 유출에 대한 소비자의 우려가 그 어느 때보다 고조되고 있다.

매년 국정감사 때마다 건강보험공단 등의 무분별한 정보 열람과 제공 및 유출 문제가 도마에 오르는 것이 그 하나의 예로 2007년 국정감사 결과에 따르면 국민연금관리공단의 경우 2006년 1~2월 2개월 동안의 특별조사 실시 결과 691명의 직원이 업무 목적 외에 총 1647건에 달하는 자료를 무단 열람한 것으로 조사되었다. 유명인사에 대한 의료기관 및 공단의 목적 외 정보 조회에서부터 불법 채권추심업자에게 8개월 동안 총 14회에 걸쳐 20여명의 재산 및 신상자료를 넘긴 건강보험공단의 직원에 이르기까지 기관의 보건의료정보의 관리 상태는 매우 심각한 수준이다. 한편 2008년 4월에는 약국 전산원이 약사의 ID를 이용하여 건강보험공단의 개인정보 72만 건을 유출하여 채권추심회사 직원들에게 넘긴 사고가 있었고, 편의상 의사 ID를 메모지에 붙여놓고 병동에서 같이 사용하는 등 의료기관 내 ID 관리도 문제로 지적되고 있다[3]-[8].

대부분의 보안사고가 그러하듯이 의료정보의 유출도 보건의료기관 내부에서의 부적절한 정보 접근이 가장 큰 원인이며 이는 정보보호관리 계획 및 지침의 부재에서 기인한다. 이러한 문제점을 최대한 극복하기 위하여 선진국에서는 개인 보건의료정보를 보호하기 위한 제도적·기술적 노력을 아끼지 않고 있다. 반면, 우리나라는

본 연구는 보건복지가족부 보건의료기술진흥사업(과제번호: A040032) 및 서울시 산학연 협력사업 (10608)의 지원으로 수행되었습니다.
* 연세대학교 의과대학 의학공학교실 (cycosxeno@gmail.com)
** (교신저자) 연세대학교 의료원 의료정보실장(knh@yuhs.ac)

선진국 수준의 보건의료정보 시스템을 구축하고 있음에도 불구하고 개인 보건의료정보의 보호에 관한 제도적·기술적 장치는 미미한 수준이다. 특히, 보건의료정보 보호관리 표준지침의 부재는 보건의료기관의 정보화 사업 및 정보자산 보호를 위한 조직의 정책수립에 혼란을 일으키고 시간과 비용 등의 문제를 야기함으로써 보안 사고의 원인이 되고 있다.

이에 본 논문에서는 보건의료 정보화 현황을 살펴보고 이러한 정보화의 안전장치로 보건의료 부문에서 추진 중인 정보보호관리 체계 표준화 동향에 대해 고찰하여 신뢰할 수 있는 보건의료정보시스템의 구축 및 운영을 위한 자료를 제공하고자 한다.

Ⅱ. 보건의료의 정보화

2.1 보건의료정보의 디지털화

보건의료 정보화의 근간은 보건의료정보의 디지털화에 있다. 진료기록의 전산화는 1991년 미 국립과학원의 요청으로 의학회(IOM: Institute of Medicine)가 발표한 'Computer-based Patient Records: an Essential Technology of Health Care'라는 보고서를 통해 본격적으로 논의되기 시작한 이래 1992년 전자의무기록협의회(CPRI: Computer-based Patient Records Institute)가 결성됨에 따라 급속히 발전하였다. 현재 미국 의학회는 정확한 자료를 제공하고 의료인에게 필요한 정보를 주어 임상결정을 도와주기 위한 병원정보시스템이나 처방전달시스템의 내부에 포함되어 있는 전자적 형태의 환자기록을 전자의무기록(EMR: Electronic Medical Record)이라고 정의하고 그 발전단계를 다음과 같이 5단계로 설명하고 있다.

2.1.1 AMR(Automated Medical Record)

의무기록의 자동화 단계로 의료보험청구를 위한 전산화 작업이라든지 환자관리를 위한 등록절차에 컴퓨터를 활용하는 등의 상태를 말한다.

2.1.2 CMR(Computerized Medical Record)

종이 의무기록의 문제로 발생되기 시작한 의무기록 보관 공간의 부족을 해결하기 위해 개발되어 기술적으로는 종이를 이용한 의무기록 자료를 단순히 이미지화하여 컴퓨터에 보관하는 수준의 단계로 종이를 이용한 차트의 구조를 크게 벗어나지 못하고 있는 형태이다.

2.1.3 EMR(Electronic Medical Record)

종이 의무기록의 완전한 디지털화(paperless)를 전제로 한 병원내의 의무기록 전산화 단계를 말한다. 의무기록을 전자적으로 활용이 가능한 형태로 보관하고 의사의 처방이 내려지면 조회 가능하되 수정 불가능한 신뢰할 수 있는 시스템이 구축 되어야 한다.

2.1.4 CPR(Computer-based Patient Record)

모든 환자의 진료정보를 필요시에 어느 병원이나 보건기관, 더 나아가 국제적으로 즉시 정보를 교류·이용하는 시스템을 말하며 사용자들에게 환자에 대한 완전하고 정확한 의무기록의 사용을 가능하게 한다. 환자에 대한 진료 방향까지 조언할 수 있는 의학지식과 연관된 전산화된 의무기록으로서 의무기록 전산화에 관련된 개념 중 가장 포괄적인 개념이라 할 수 있다.

2.1.5 EHR(Electronic Health Record)

병원 간, 국가 간의 정보 교류가 환자의 의료적인 부분뿐만 아니라 한 사람의 건강에 관한 모든 문제를 포괄하는 광의의 개념이다. 병원이 환자 스스로 건강관리가 가능하도록 지원한다.

이러한 5가지 개념 중 최상위 단계인 EHR은 최근 서비스 제공자 중심이 아닌 개인 중심의 서비스로 의료서비스 패러다임이 변화하면서 PHR(Personal Health Record)로 다시금 진화하고 있다.

2.2 보건의료정보화 현황

2.2.1 국내 의료기관의 정보화

병원정보시스템은 1960년대 중반에 미국과 네덜란드, 스웨덴, 스위스와 같은 몇몇 유럽 국가들에서 처음 개발되었다. 우리나라는 1977년 건강보험 제도가 시행되면서 보험환자들의 진료비 청구로 업무가 복잡해지고 환자가 증가하게 되자 원무행정 중심으로 병원 전산화

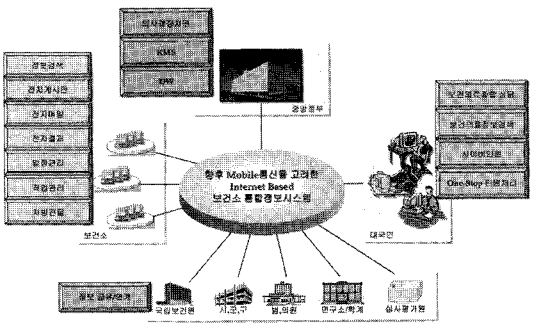
가 이루어졌다. 국내에서 병원정보시스템의 개발이 시도된 것은 1978년 경희의료원에 건강보험 업무를 위한 미니컴퓨터가 설치 운영되면서부터이다. 이후 1979년에 서울대학부속병원에서 대형컴퓨터를 설치 가동하였으며 현재는 정도의 차이는 있지만 대부분의 의료기관에서 EDI(Electronic Data Interchange), OCS(처방전달시스템: Order Communication System), PACS(영상저장전달시스템: Picture Archiving and Communication System), EMR(전자의무기록)시스템 등의 병원정보시스템을 운영하고 있다.

[표 1]은 2005년 건강보험심사평가원이 전국의 요양기관을 대상으로 조사한 정보화 실태조사의 결과이다. 2005년을 기점으로 본격적인 병원 정보화 사업이 진행되었음을 고려할 때 현재의 정보화 현황과는 그 데이터에 많은 차이가 있겠으나 2005년 조사에서 이미 EDI, OCS, PACS는 성숙기에 도달하였고 EMR의 경우 의원에서 오히려 더 많이 채택하고 있음을 알 수 있다.

의료기관의 정보화는 전자적인 진료정보 교류의 가능성을 증대시키고 있다. 진료정보를 타 기관과 공동으로 활용하기 위해서는 앞서 언급한 의무기록의 전산화 과정 중 제3단계인 EMR시스템 구축이 전제되어야 한다. 국내에서는 2000년대 초중반부터 삼성의료원, 인하대학교 병원, 대구 동산의료원, 서울대학교 분당병원, 세브란스병원 등 대형 종합병원을 중심으로 단위병원에 맞춤화한 EMR시스템이 구축되어 왔고 중소병의원의 경우 비트컴퓨터, 의사랑, 이수유비케어 등 몇몇 업체에서 개발한 EMR시스템을 채택하여 사용하고 있다.

2.2.2 국가 보건의료정보화 사업

의료시스템 운영의 합리화 및 의료서비스 질 향상을 위해 도입된 진료전달체계 및 의료기관 간 자율적인 협력체계에는 효율적인 진료정보의 교류가 필수적이다. 보건복지부는 1998년 '21세기 보건의료 발전 종합계획'을 수립하면서 평생국민건강관리체계 구축, 수요자 중심의 보건의료공급체계 구축, 보건의료산업의 경쟁력 제고, 보건의료 선진화의 기반 조성을 4대 기본목표로 삼았다. 세부 실행과제로 2001년 '보건의료정보 공동활용을 위한 기본계획'이 수립된 이후, 진료정보 공동활용을 위한 시범사업 모델이 제시되었고 '질환유전체 지식시스템', '에이즈 감시 정보시스템', '전염병 감시정보시스템' 등 다양한 질병 감시관리 통합 시스템이 구축·운영되고 있다. 특히, 2004년부터 지역 주민의 평생전자건강기록(EHR: Electronic Health Record)을 관리하기 위한 '보건소 간 주민 건강정보 공동 활용 시스템'이 [그림 1]과 같이 설계되어 2007년 하반기부터 전국 규모로 확대 운영되고 있으며 2007년부터 공공의료기관의 진료정보 교류 시스템이 일부 구축·시범 운영 중이다.



〔그림 1〕 보건소 통합정보시스템 구성도[10]

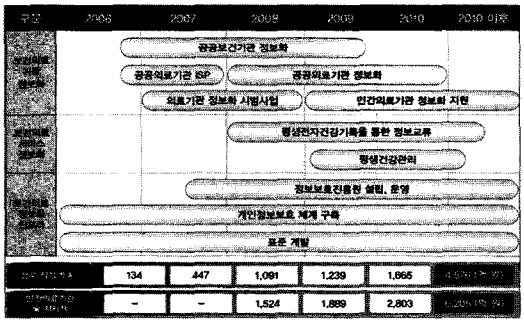
〔표 1〕 2005년 요양기관 정보화 실태조사[9]

구분	종합전문병원	종합병원	병원	의원
전체의료기관 수	42개	249개	903개	25,145개
응답률	100%	31.3%	22.6%	14.4%
EMR	21.6%	16.4%	24.4%	43.3%
PACS	92.5%	82.5%	23.3%	3.2%
OCS	100.0%	87.1%	67.5%	43.3%
EDI	100.0%	100.0%	89.9%	39.9%

이러한 국가 보건의료정보화 사업의 중심에는 지난 2005년 12월 출범한 '보건의료정보화사업 추진단'과 인프라를 개발하는 'EHR 핵심공통기술연구개발사업단'이 있으며 [그림 2]와 같은 비전으로 2010년까지 원하는 국민 모두가 전자건강기록을 통해 언제 어디서나 질 높은 의료서비스를 이용할 수 있는 시스템 제공에 1조 800여억 원의 비용이 투자될 계획이다.

2.2.3 해외의 국가 보건의료정보화 사업

병원 간, 국가 간 경계를 넘어선 지속적인 건강관리 시스템 구축을 위하여 세계 각국은 국가 보건의료정보

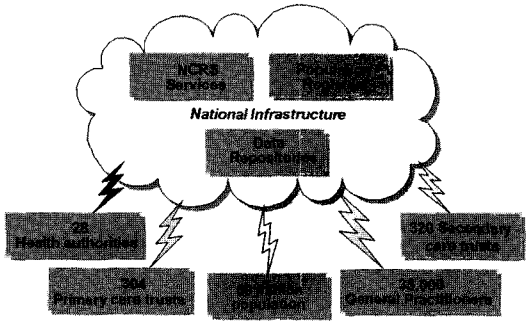


〔그림 2〕 국가 보건의료정보화 사업 로드맵[11]

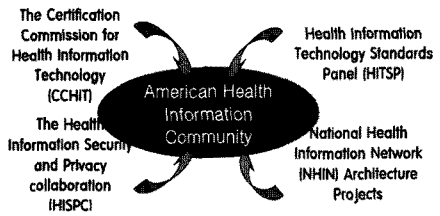
화 구축 사업에 노력을 기울이고 있다. 영국은 2001년부터, 캐나다와 미국, 호주는 각각 2004년부터 국가 단위의 보건의료정보화 사업을 장기계획으로 추진하고 있다.

영국의 경우 1997년 토니 블레어 총리의 현대화 전략에 따라 전통적으로 무료로 제공되어 왔던 NHS (National Health Service)의 개선이 시작되어 지역 보건의료 정보화에 기반을 둔 국가 통합 보건의료망을 지향하며 2001년부터 2010년까지 약 11조 3000억 원을 투입하는 국가사업(NPfIT: National Programme for IT)이 진행 중이다. 의료기록을 기본으로 하는 영국의 보건의료정보화는 전자의무기록의 형태로서 CPR과 EHR을 바탕으로 환자의 기록정보에 부합하는 맞춤형 치료와 인터넷 네트워킹을 통한 의료정보 전달 서비스의 제공을 목적으로 한다.

한편 2004년 4월 27일 미 대통령 부시는 대통령령 13335에서 의료비절감, 의료사고 및 오진 예방, 의료서비스의 질 개선을 목적으로 10년 이내 모든 국민의 의무기록전자화를 골자로 하는 의료정보화계획을 공포하였다. 이에 미 정부는 2004년부터 2010년까지 100조 원 이상의 대규모 비용을 투입하는 국가 보건정보망 구축 사업(NHIN: Nationwide Health Information Network)



〔그림 3〕 NPfIT vision for virtual health[12]



〔그림 4〕 미국 국가 보건의료정보화 구축 협력체계[13]

을 진행 중이다. 전담 기구인 NCHIT(National Coordinator for Health Information Technology)는 전국적인 보건의료 네트워크 아키텍처 구축단 및 다양한 협력체와 함께 법제도적 문제, 운영 고려사항, 개인정보 보호를 위한 기준과 자료교환 방식, 전자건강기록 인증 방식 등의 표준 및 상호운용성 기준을 마련하고 있다. [그림 4]는 이러한 협력체계를 나타낸다.

Ⅲ. 보건의료의 정보보호관리 체계

이상에서 국내외의 보건의료정보화 현황에 대해 살펴보았다. 본 장에서부터는 정보화의 안전장치로 보건의료부문에서 추진되고 있는 정보보호관리 체계 준비 동향을 고찰하고자 한다.

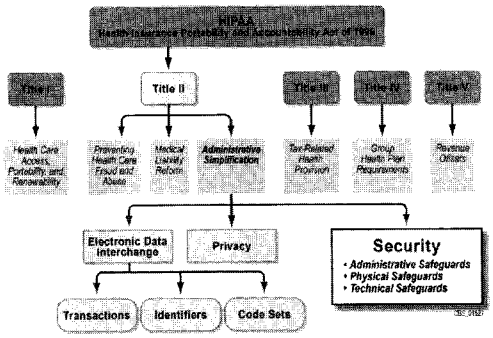
정보보호관리 체계란 조직 자산의 안정성과 신뢰성을 향상시키기 위한 절차를 체계적으로 수립하고 문서화하여 지속적으로 관리·운영함으로써 정보의 기밀성, 무결성, 가용성을 실현하기 위한 일련의 과정과 활동에 관한 표준이라 할 수 있다. 국제 표준인 ISO27001, ISO27002, ISO13335와 한국정보보호진흥원(KISA)의 ISMS(Information Security Management System) 등 일반 조직의 자산 보호와 시스템 운영을 위한 관리 표준은 이미 마련되어 안정기에 이르렀고 또 새로운 환경에 맞추어 진화하고 있다. 그러나 보건의료부문은 보호대상 자체가 일반적인 정보자산보다 더욱 민감한 정보이고 조직의 프로세스도 일반 사업체와는 차별되는바 의료정보 선진국인 미국을 중심으로 보건의료분야에 특화된 정보보호관리 표준이 개발 중이며 국내에서도 이러한 연구가 시도되고 있다.

3.1 HIPAA Security Rule

미국의 의료보험과 관련하여 보건의료정보의 교환과 책임에 관해 규정하고 있는 HIPAA(Health Insurance

Portability and Accountability Act, 1996)는 공법 104-191로 1996년 8월 제정되었다. HIPAA는 [그림 5]와 같이 의료서비스 접근 호환 및 갱신(Title Ⅰ) 건강관리의 남용예방, 행정 간소화, 의료책임 개혁(TitleⅡ), 조세관련 법규(TitleⅢ), 단체의료보험 집행(TitleⅣ), 수입상쇄(TitleⅤ)로 구성되어 있는데 TitleⅡ의 F항 행정 간소화에서 EDI, 프라이버시, 보안을 규정하고 있다.

HIPAA Security Rule은 전자문서 형태의 보건의료정보의 기밀성, 무결성, 가용성을 보호하기 위한 규정으로 의료보험기관, 의료서비스 제공자(병원, 클리닉, 공공 보건기관, 의료인 등), 그 외 건강관리 프로그램 등이 그 적용 대상이다. 미 보건복지부(HHS)는 HIPAA의 요구에 의해 개인을 식별할 수 있는 보건의료정보를 보호하기 위한 프라이버시 규정(Privacy Rule)을 마련하여 2000년 공포하면서 이 법의 적용을 받는 조직은 적절한 보안장치를 마련할 것을 강제했다. 이러한 요구에 의해 관리적, 기술적, 물리적 보안장치에 관한 표준(Standard)과 이행



〔그림 5〕 HIPAA Component

명세(Implementation Specification)를 서술한 Security Rule이 선포되어 2003년 4월부터 일부 시행되었고 2006년 4월부터 전체 조항이 시행되고 있다. Security Rule을 위반할 경우, 개별 요구사항마다 $100의 벌금을 부과하되 모든 위반 사항을 합쳐 $250,000를 초과할 수 없으며 식별 가능한 보건의료정보의 유출 시 $50,000의 벌금과

〔표 2〕 HIPAA Security Standard Matrix

보안조항	표준	이행 명세
관리적 보안 조항 §164.308	보안관리	위험분석(필수), 위험관리(필수), 제재정책(필수), 정보시스템 활동 검토(권고)
	보안담당자 확보	none
	작업장 보안	피고용인 인증 및 감독(권고), 작업장 접근 절차(권고), 작업장 접근 종료 절차(권고)
	정보접근 관리	의료정보센터의 접근정책과 절차(필수), 접근승인(권고), 접근군한 수립과 변경(권고)
	보안의식 및 훈련	보안갱신(권고), 바이러스보안(권고), 로그인 모니터링(권고), 패스워드 관리(권고)
	보안사고 처리절차	보안사고 보고(필수)
	비상계획	데이터백업계획(필수), 데이터복구계획(필수), 비상시 운영계획(필수), 테스트와 개정절차(권고), 애플리케이션과 데이터 중요성 평가(권고)
	평가	none
	협력기관 계약과 기타 협정	서면계약과 협정(필수)
물리적 보안 조항 §164.310	시설접근 통제	비상운영(권고), 시설보안계획(권고), 접근통제와 확인절차(권고), 유지보수 문서화(권고)
	워크스테이션 이용	none
	워크스테이션 보안	none
	매체 통제	매체폐기(필수), 매체재사용(필수), 매체이동 문서화(권고), 데이터백업 및 저장(권고)
기술적 보안 조항 §164.312	접근 통제	인적사항확인(필수), 비상접근절차(필수), 자동로그오프(권고), 암호 및 복호화(권고)
	감사 통제	none
	무결성	무결성절차(권고)
	사람 또는 개체 인증	none
	전송 보안	무결성통제(권고), 암호화(권고)

1년 이하의 징역, 의도적인 유출의 경우 $100,000의 벌금과 5년 이하의 징역, 그리고 판매 목적의 유출 시 $250,000의 벌금과 10년 이하의 징역을 양형할 수 있다[14],[15]. HIPAA Security Rule은 보건의료정보의 취급에 대한 표준을 제공함으로써 실무자의 이해를 도모하고 개인의 프라이버시 통제권을 보장하여 질 높은 건강관리 서비스를 제공하는 데 그 목적이 있다. HIPAA Security Rule은 총 3개의 보안조항(Security Safeguard)과 18개의 표준항목(Standard), 20개의 필수 이행 명세(Required Implementation Specification), 그리고 22개의 권고 이행 명세 (Addressable Implementation Specification)로 구성되어 있다.

그 가운데 관리적 보안이 9개 표준항목, 12개 필수 이행 명세, 11개의 권고 이행 명세를 규정하고 있어 전체 규정의 55%를 차지한다. 물리적 보안은 4개 표준항목, 4개 필수 이행 명세와 6개의 권고 명세로 전체 규정의 24%, 기술적 보안은 5개 표준항목과, 4개 필수 이행 명세, 5개의 권고 이행 명세를 서술하고 있어 21%의 분포를 보이고 있다. 권고는 선택과 동일한 의미가 아니며, 필수적으로 요구되는 사항이지만 여러 가지 이유로 준수할 수 없을 때에 한해 준수하지 않아도 된다는 의미다. 이때에는 반드시 타당한 이유를 문서화하여 제시해야 한다[16].

3.2 HL7 EHR WG

3.2.1 EHR시스템 기능 모델

HL7(Health Level 7)은 다양한 보건의료정보시스템 간 정보의 교환을 위해 미 국립표준연구소(ANSI: American National Standard Institute)가 인증한 표준 및 표준 조직으로 미국뿐 아니라 전 세계적으로 가장 널리 쓰이고 있는 보건의료정보의 표준이다. HL7에는 다양한 워킹그룹(WG: Working Group)이 형성되어 보건의료정보 표준에 관한 연구를 하고 있다. HL7 EHR WG은 2003년 4월 EHR 기능 명세를 발표한 이후 보완을 계속하여 2007년 2월 ANSI 표준으로 "HL7 EHR System Functional Model, Release 1"을 발표했다. 이들은 EHR시스템의 기능을 진료, 진료지원, 정보인프라로 분류하고 각 기능별 하위 2~3단계로 세분화하여 각각에 대해 번호, 유형, 명명, 정의·내용, 참조, 적용항목을 명시하였다. 정보의 보호관리는 정보인프라를 구성하는 7가지 기능 가운데 보안(IN.1), 정보관리(IN.2)에서 [표 3]과 같이 총 14개의 기능으로 세분하여 정의되고 있다.

〔표 3〕 HL7 EHR-S Functional Model[17]

기능	세부기능	세세부 기능
IN. 정보 인프라	IN.1 보안	IN.1.1 개체 인증
		IN.1.2 개체 권한관리
		IN.1.3 개체 접근통제
		IN.1.4 환자 접근관리
		IN.1.5 부인방지
		IN.1.6 안전한 데이터 교환
		IN.1.7 안전한 데이터 라우팅
		IN.1.8 정보의 증명
		IN.1.9 환자 프라이버시/비밀 보호
	IN.2 정보관리	IN.2.1 데이터 보관, 이용, 파기
		IN.2.2 감사 기록
		IN.2.3 동기화
		IN.2.4 건강기록정보의 추출
		IN.2.5 정보의 저장 관리

3.2.2 PHR시스템 기능 모델

의료서비스의 패러다임이 의료기관 중심에서 소비자 중심으로 변화되면서 보건의료정보도 병원에서 생성된 진료기록 중심의 EHR에서 개인 중심의 평생 건강관리 개념인 PHR(Personal Health Record)로 진화하고 있다. 이에 HL7 EHR WG은 PHR시스템의 기능 모델(안)을 2007년 8월 발표하고 1년 이상의 공개를 거쳐 수렴한 의견을 바탕으로 새롭게 보완한 안을 2008년 12월에 다시 발표하였다. 이들은 PHR의 기능을 개인건강, 건강지원, 정보인프라로 분류하고 각각을 다시 2~3단계로 분류하였는데 건강정보의 보호관리 부분은 정보인프라를 구성하는 4가지 기능 가운데 상호운용 표준에 관한 부분을 제외하고 [표 4]와 같이 건강기록정보의 관리, 보안, 감사기록의 3가지 하위 기능에서 다뤄지고 있다.

3.3 CCHIT-EHRs Security Criteria

CCHIT(Certification Commission for Healthcare Information Technology)는 2004년 7월, 미국의 3대 의

〔표 4〕 HL7 PHR-S Functional Model[18]

기능	세부기능	세세부 기능
IN. 정보 인프라	IN.1 정보관리	IN.1.1 데이터 관리
		IN.1.2 동기화
		IN.1.3 Ad Hoc 조회
		IN.1.4 건강기록정보의 추출
		IN.1.5 비구조화된 정보의 저장 관리
		IN.1.6 구조화된 정보의 저장 관리
		IN.1.7 환자기록 디렉토리 서비스
		IN.1.8 용어 표준
		IN.1.9 용어 표준의 버전 관리
		IN.1.10 용어 매핑
		IN.1.11 비즈니스 규칙의 관리
		IN.1.12 업무 관리
	IN.3 보안	IN.3.1 개체 인증
		IN.3.2 개체 권한관리
		IN.3.3 개체 접근통제
		IN.3.4 부인방지
		IN.3.5 안전한 데이터 교환
		IN.3.6.안전한 데이터 라우팅
		IN.3.7 정보 보관
		IN.3.8 환자 프라이버시/비밀 보호
		IN.3.9 서비스 가용성
		IN.3.10 안전한 메시지 교환
	IN.4 감사 기록	

〔표 5〕 CCHIT EHR시스템 보안 기준[19],[20]

번호	WG	항목/내용
S1~S4	Sec	Security : 접근통제
S5~S11	Sec	Security : 감사
S12~22	Sec	Security : 인증
S23	Sec	Security : 문서화
S24~S30	Sec	Security : 기술서비스
S31	Sec	Security : 인증 (2009년 이후)
S32~S33	Sec	Security : 기술서비스 (2009년 이후)
S34~36	Sec	Security : 접근통제 (2008년 이후)
S37	Sec	Security : 감사 (2009년 이후)
R1~R3	Sec	Reliability : 백업/복구
R4~R13	Sec	Reliability : 문서화
R14~R15	Sec	Reliability : 기술서비스
R16	Sec	Reliability : 문서화(2007년 이전)
R17	Sec	Reliability : 기술서비스(2007년 이전)
R18	Sec	삭제 (S23과 병합)
R19	Sec	삭제

료정보기술 산업협회인 의무기록협회(AHIMA: American Health Information Management Association), 의료정보관리시스템협회(HIMSS: Healthcare Information & Management Systems Society), 국가의료정보기술연합(NAHIT: National Alliance for Health Information Technology)이 보건의료정보 시스템의 인증을 위해 자율적으로 결성한 민간조직으로 2005년부터 미 보건복지부(HHS)와 계약을 맺고 국가 보건의료정보화 사업(NHIN)에 협의체로 활동하고 있다. 이후 2006년 5월과 2007년 3월에 외래환자용 EHR시스템(EHRs) 인증기준을 발표하였고 2007년 6월에는 입원환자용 EHRs 인증기준을 발표하였다. 2008년 현재 CCHIT는 소아외래환자용, 심혈관계외래환자용 EHRs에 대한 인증기준을 개발 중이다. CCHIT EHRs 인증기준은 EHRs의 기능성, 상호운용성, 보안성 항목으로 구성되어 있으며 명세서는 번호, 워킹그룹, 항목/내용, 세부기준, 참조, 범례로 이루어져 있다.

EHRs 보안 인증기준은 ISO17799, HIPAA Security 표준, 캐나다 앨버타주의 벤더 적합성 및 유용성 요구사항(VCUR) 표준, ISO/IEC15408, NIST 800-53, 캐나다 온타리오주의 의료협회 표준 등을 참고하여 작성되었고 크게 보안성과 신뢰성 항목으로 구성된다. 2007년 5월, 2008년 5월, 2009년 5월 이후 기준으로 각각 이전, 신규, 수정으로 범례를 표시하여 같은 항목에 대해서도 그 적용 시점에 따라 번호를 달리 표현하였으며 병합 또는 삭제된 항목도 해당 번호를 지우지 않고 그대로 유지하고 있는 것이 특징이다. 2007월에 발표한 EHRs 보안 인증기준은 그 항목이 외래환자와 입원환자에 모두 동일하다. [표 5]는 CCHIT의 EHRs 보안 인증기준 항목을 나타낸 것이다.

3.4 보건복지가족부 EHR핵심공통기술연구개발사업단의 개인건강정보 보안 체계

한국의 국가 보건의료정보화 사업 추진체계인 EHR 핵심공통기술연구개발사업단(이하 EHR사업단)은 국가 보건의료정보화 사업 계획에 따라 2006년부터 개인건강정보 보호를 위한 프라이버시와 보안(P&S) 체계 와 지침을 개발하고 있다. 2009년 3월에 3년간의 성과물을 발표할 예정이며 2008년 12월 EHR사업단의 보고서에 따르면, ISO27001의 도메인 체계에 JIS Q15001, KISA

〔표 6〕 EHR사업단 개인건강정보 보안 체계(안)[21]

영역	항목/내용
1. 의료정보보호 정책	1.1 의료정보보호정책문서 1.2 의료정보보호정책 유지관리
2. 의료정보보호 조직	2.1 내부조직 2.2 외부자 조직
3. 정보자산분류	3.1 자산관리 책임 3.2 정보분류
4. 인적자원	4.1 고용시 점검사항 4.2 직무수행 관리 4.3 퇴직 및 직무변경 4.4 정보보호 교육 및 훈련
5. 물리적, 환경적 보안	5.1 보안구역 5.2 의료정보시스템 기기보안
6. 통신 및 운영관리	6.1 운영절차 및 책임 6.4 유해소프트 및 모바일코드로부터의 보안 6.7 매체관리 6.8 의료정보의 교환 6.9 모니터링
7. 접근통제	7.1 접근통제에 대한 업무 요구사항 7.2 사용자 접근관리 7.3 사용자 책임 7.4 네트워크 접근통제 7.5 운영체제 접근통제 7.6 AP 접근통제 7.7 이동컴퓨팅 원격지 근무
8. 시스템 도입, 개발, 유지보수	8.1 정보시스템 보안 요구사항 8.2 어플리케이션의 정확한 처리 8.3 암호화 통제 8.4 시스템 파일 보관 8.5 개발 및 지원 과정에서의 보안 8.6 기술적 취약점 관리
9. 침해사고 관리	9.1 보안사고 대응체계 수립 9.2 침해사고 대응 및 사후관리
10. 업무 연속성 계획	10.1 사업연속성 관리의 정보보호 측면
11. 준거성	11.1 법적 요구사항에 대한 부합성 11.2 보안정책, 표준 및 기술적 부합성 검토 11.3 보안감사 고려사항

의 ISMS 등을 참고하여 총 11개 영역, 138개 통제항목을 도출하고 각 항목에 대해 목적과 부항목을 작성 중이다. [표 6]은 진행 중인 EHR사업단의 개인건강정보 보안 체계 주요 명세(안)이다.

Ⅳ. 결 론

보건의료정보는 그 특성상 개인의 통제를 벗어나 수집·이용·공개될 경우, 사회적 차별의 원인이 되거나 개인의 기본적 인권을 현저하게 침해할 우려가 있는 요주의 정보이다. 과거에는 보건의료정보가 병원이나 보건소에서 수집되어 해당 기관의 의무기록실에 문서로 보관되어 있었으나 현재는 모든 보건의료기록이 전자화된 네트워크를 통해 기관 내·외부로 전송, 공동 관리됨과 동시에 국민 평생건강정보를 통합 관리할 수 있는 시스템이 구축되는 과정에 있다. 이러한 시스템을 운영하기 위해 충족되어야 할 전제조건은 보건의료정보의 관리를 위한 표준화된 지침의 마련이다. 일반 정보와 개인을 식별할 수 있는 정보가 각각 분리해서 관리되어야 하고 정보의 표준화와 함께 정보의 보호·관리에 관한 표준화가 이루어져야 한다. 이러한 표준은 국민의 정보 자기통제권을 보장해 줌으로써 정보유출에 대한 국민적 우려를 감소시킬 수 있을 뿐 아니라, 보건의료정보 취급조직에게는 실행의 지침이 된다.

본 논문은 보건의료 부문의 정보화를 파악하고 정보화의 편익과 함께 공존하는 역기능을 효과적으로 관리하기 위한 대책으로 여러 기구에서 제정되었거나 현재 개발 중인 보건의료정보 보호관리 체계에 대해 살펴보았다. 대국민 서비스의 향상과 기관의 업무 효율성 향상, 그리고 정보의 축적에 따른 지식 정보화를 가능케 하는 주요 수단으로 보건의료정보시스템이 공공부문과 민간부문에서 빠르게 확산되고 있는 반면, 그에 따른 법제도나 정보의 보호·관리를 위한 체계는 미비한 상황임을 알 수 있다. 보건의료정보는 개인의 가장 민감한 정보로 최상의 보호가 이뤄져야하는 한편 국민 건강과 복지 향상을 위한 공익의 성격도 강하여 관리와 책임에 대한 명확한 지침이 더욱 절실하다. 개인과 국가의 자산인 보건의료정보를 안전하게 보호하고 효과적으로 관리하기 위한 지침과 그 시스템에 대한 인증 체계 마련이 시급하다.

참고문헌

[1] 보건복지부, 2007년도 보건복지정보화촉진시행계획(안), 2007.

[2] 보건의료기본법 (2008.03.28 법률 제9034호).

[3] "건보공단서 내 개인정보 줄줄 새고 있다", 이헬스뉴스, 2006.10.18.

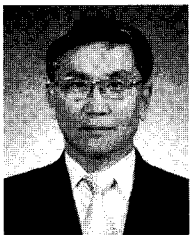
[4] "건보·연금공단 직원, 국민 개인정보 유출 심각해 친구 애인·여동생 남자친구 뒷조사까지", 조선일보, 2007.9.27.

[5] "국민연금공단, 유명연예인 정보 무단 열람", 조선일보, 2008.8.5.
[6] "약사인증서 · 비밀번호 이용 건강보험공단 개인정보 72만건 유출..채권추심원에 넘겨", 연합뉴스, 2008.4.11.
[7] "병원.약국 1만 4천명 개인정보 유출", MBC TV, 2006.10.24.
[8] "누군가 당신 병력을 본다면 … 대형병원 전자의무기록 접근 쉬워", 중앙일보, 2005.6.23.
[9] 건강보험심사평가원, 요양기관 정보화 실태조사, 2005.
[10] 舊보건복지부, 보건의료정보화 촉진 계획, 2005.
[11] 舊보건복지부, 보건복지 정보화 촉진 시행계획, 2007.
[12] HP, NPfIT Vision for virtual healthcare, 2004.
[13] 부유경, "미국 보건의료정보화 추진 현황", EHR 핵심공통기술연구개발 사업단, 2006.
[14] U.S. HHS, 45 CFR Parts 160, 162 and 164 Health Insurance Reform: Security Standards; Final Rule, Feb 2003.
[15] U.S. HHS, Summary of the HIPAA Security Rule, Office for Civil Rights, 2003.
[16] 정혜정, "보건의료기관의 정보보호관리 표준지표 개발", 표준화우수논문 수상논문집, 한국표준협회, pp. 215-267, 2005.
[17] HL7 EHR TC, EHR-S Functional Model, Release 1, Health Lever 7, February 2007.
[18] HL7 EHR TC, PHR-S Functional Model, Release 1, HL7 DSTU Release 1, Health Lever 7, Dec 2008.
[19] CCHIT, Final Security Criteria for 2007 Certification of Ambulatory EHRs, 2007.3.16.
[20] CCHIT, Security Criteria for 2007 Certification of Inpatient EHRs Final, 2007.6.28.
[21] EHR핵심공통기술연구개발사업단, 개인건강정보의 보안체계, EHR핵심공통기술심포지엄, pp. 33-46, 2008.12.
[22] 한국정보보호진흥원, 지식정보사회 의료 패러다임 변화와 정보보안, 정보보호 정책동향, 2006.
[23] Pauline Bowen, Arnold Johnson, Joan Hash, Carla Dancy Smith, Daniel I. Steinberg, "Information Security: An Introductory Resource Guide for Implementing the HIPAA Security Rule", NIST, 2004.
[24] NIST, Managing Risk from Information Systems, NIST SP 800-39, 2008.

〈著者紹介〉

정 혜 정 (Hye-Jeong Jeong)
정회원

1996년 2월: 연세대학교 간호학과 학사
2005년 8월: 연세대학교 정보대학원 석사
2009년 2월: 연세대학교 대학원 의료정보 박사
2003년~현재: 연세대학교 의과대학 의학공학교실 선임연구원
2005년~현재: 유비쿼터스 의료허브 구축 사업단 간사
<관심분야> 의료정보, u-Health, 정보보호, 법제도



김 남 현 (Nam-Hyun Kim)

1977년 2월: 연세대학교 공과대학 전기공학과 학사
1982년 2월: 연세대학교 대학원 전기공학과 석사
1987년 2월: 연세대학교 대학원 전기공학과 박사
1990년~현재: 연세대학교 의과대학 의학공학교실 교수
2008년~현재: 연세대학교 의료원 의료정보실 실장
<관심분야> 의료정보, u-Health, 의료기기, 생체계측