보건의료정보 보호관리 모델 개발†

정혜정*, 김남현*
*연세대학교 정보대학원 의료정보학과
e-mail:xeno@yonsei.ac.kr

Information Security Management in Healthcare Area

Hey-Jeong Jeong*, Nam-Hyun Kim*
*Graduate School of Information, Yonsei University

요 약

보건의료정보는 개인의 가장 민감한 정보로 최상의 보호가 이뤄져야하는 한편, 국민 건강과 복지 향상을 위한 공익의 성격도 강하여 관리와 책임에 대한 명확한 지침이 반드시 필요하다. 본 연구에서는 보건의료 부문의 특성과 정보화 현황을 반영하고 선행연구의 한계점을 보완하여 국내 보건의료 환경에 적합한 정보보호관리 모델을 개발하였다. BS7799, HIPAA Security Rule, HL7 EHR SIG 기능명세 등을 참고하여 필요성, 정보보호 목적/전략 수립, 위험분석/평가, 정보보호관리 정책수립, 정보보호관리 프레임워크 설계, 관리적 보안, 물리적 보안, 기술적 보안, 정보보호관리 평가, 운영관리의 총 10개 세부 프로세스와 111개의 이행지표로 구성된 본 모델은 보건의료정보 취급자에게 실행 지침을 제공하여 보건의료정보시스템의 안전성 향상과 국민 보건복지 수준 향상에 이바지할 수 있을 것으로 기대된다.

1. 서론

보건의료기본법에 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 자료로 일반 개인정보와 차별화하여 정보 수집을 제한하고 있는 민감한 정보다. 보건의료정보가 당해 의료기관 내에서 수집·이용되는 것에 그치지 않고 언제 어디서나 수집되어 기관 간, 국가 간에 전자적으로 교환 및 활용되는 환경에서 개인의 자기 정보 통제는 점점 더 어려워지고 있다. 이러한 문제점을 최대한 극복하기 위하여 선진국에서는 개인 보건의료정보를 보호하기 위한 제도적·기술적 노력을 아끼지 않고 있다. 반면, 우리나라는 선진국 수준의 보건의료정보 시스템을 구축하고 있음에도 불구하고 개인 보건의료정보 보호관련 장치는 미미한 수준이다. 특히, 보건의료정보 보호관리 체계의 부재는 보건의료기관의 정보보호 정책수립에 혼란을 일으키고 시간과 비용 등의 문제를 야기할 뿐만 아니라 개인의 정보보호 유출에 대한 우려를 유발함으로써 시스템 활성화의 핵심 장애요소로 작용할 위험이 있다.

이에 본 연구에서는 신뢰할 수 있는 보건의료정보시스템의 구축과 운영을 통해 국민 복지를 향상시키고 도래하는 유비쿼터스 헬스케어 환경에서 국가적인 경쟁력을 높일 수 있는 보건의료정보 보호관리 모델을 제시하고자 한다. 이를 위하여 국내 보건의료정보 보호관리 현황을 분석하여 문제점과 요구사항을 도출하고 다양한 선행연구 고찰을 통해 국내 환경에 적합한 보건의료정보 보호관리 모델을 개발하였다.

2. 보건의료정보 보호관리 현황

현재 국내에는 보건의료기관에서 생성되는 정보를 다룸에 있어서 통일된 지침없이 개별 기관마다

† 본 연구는 보건복지부 휴대형 진단치료기기 개발센터 (0405-ER01-0304-0001) 지원으로 수행되었음

상이한 내부지침에 의존하고 있다. 김옥남(2003)이 5개 대형 의료기관을 대상으로 내부 의무기록 접근권한 현황을 조사한 결과에 따르면 의과대학 학생, 인턴 등을 제외한 대부분의 보건의료종사자가 모든 의무기록에 자유롭게 접근할 수 있으며 의과대학 학생에게 조차 접근이 개방된 병원도 있었다. 정보 접근 가능기간에 대해서도 대부분 제한이 없었으며 접근 방법으로는 가장 낮은 수준의 인증 방법인 ID와 Password 인증이 일반적이었다.[2] 기관 간 진료정보 공동활용은 삼성의료원, 대구동산의료원, 서울아산병원 등 몇몇 대형 종합병원 중심으로 각각 하위기관과 일부 진료정보를 교환하거나 서울대병원과 서울대분당병원처럼 상호 대등한 관계로 정보를 연계하는 형태로 이뤄지고 있다. 그러나 기관 간 자유로운 정보 공유가 제도적으로 보장되어 있지 않은데다 시스템 개발에 대한 통일된 지침과 모범사례마저 없어 보건의료정보를 보호하기 위한 절차나 대책은 우선순위에서 밀려나고 있는 것이 사실이다. 선진국에서 보건의료기관의 시스템에 대해 사전 프라이버시 영향평가를 실시하는 것과는 대조적이다. 2004년 5월, 연세대학교 보건학과에서 80개의 의료기관을 대상으로 실시한 진료정보 공동활용을 위한 설문조사 결과에 따르면 우선적으로 해결되어야 할 과제로는 표준화와 개인정보 노출에 따른 보안문제가 가장 높은 순위를 차지하였다.[4]

3. 보건의료정보 보호관리 체계 고찰

이상 보건의료 정보화와 정보관리 현황 및 그 문제점에 대해 살펴보았다. 본 장에서는 보건의료정보 보호표준을 고찰하여 국내 보건의료정보환경에 적합한 모델 개발의 근거를 제시하고자 한다.

(1) HIPAA 보안 규정 (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.[8][19] 미 보건복지부(HHS)는 HIPAA의 요구에 의해 개인을 식별할 수 있는 보건의료정보를 보호하기 위하여 관리적, 기술적, 물리적 보안장치에 관한 표준(Standard)과 보건의료정보의 의도적 또는 비의도적 사용과 표준에 위반되는 유출로부터의 합리적인 보호를 위한 이행 명세(Implementation Specification)를 서술한 보안 규정(Security Rule)을 2003년 4월 선포하였다. HIPAA 보안 규정은 전자 형태의 보건의료정보의 기밀성, 무결성, 유효성을 보호하기 위한 규정으로 의료보험기관, 건강관리 제공자, 보건의료정보 취급 조직이 그 적용 대상이다. HIPAA 보안 규정은 총 3개의 보안 조항(Security Safeguard)과 18개의 표준항목(Standard), 20개의 필수 이행 명세(Required Implementation Specification), 그리고 22개의 권고 이행 명세 (Addressable Implementation Specification)로 구성되어 있다.[20] 그 가운데 관리적 보안이 9개 표준항목, 12개의 필수 이행 명세, 11개의 권고 이행 명세를 규정하고 있어 전체 규정의 55%를 차지한다. HIPAA 보안 규정은 보건의료정보의 보호관리에 관하여 대표성을 띄는 표준이지만 정보 보안 요구사항에 부합하는 표준 프로세스와 상세한 지침을 제공하고 있지 않고 권고 조항에 관한 명확한 기준이 없어 실무에 적용 시 어려움이 많다.

(2) HL7 EHR SIG의 EHR 기능 명세

HL7(Health Level 7)은 다양한 보건의료정보시스템 간 정보의 교환을 위해 미국 국립표준연구소(ANSI: American National Standard Institute)가 인증한 표준으로 미국뿐 아니라 전 세계적으로 가장 널리 쓰이고 있는 보건의료정보의 표준이자 표준을 제정하는 조직을 의미한다. HL7 EHR SIG는 2003년 4월 HL7 이사회로부터 EHR 시스템의 기능적 모델 개발에 대한 승인을 얻어 의료 환경을 진료관리, 임상 의사결정 지원, 운영관리 및 의사소통, 임상 지원, 측정/분석/연구 및 보고, 원무, 정보 인프라의 7개 기능으로 분류하였다. 각 기능별로 하위 기능을 2단계로 상세 분류하고 각 기능에 대해 명세(Statement), 서술(Description), 근거(Rationale)를 정의하였다. 정보보호관리 부분은 정보 인프라(Information Infrastructure - I.1)를 구성하는 8가지 기능 가운데 EHR 정보 보안(I.1.1.0), EHR 정보 관리(I.1.2.0)에서 다루고 있다.[9] 그러나 HL7 EHR SIG 기능 명세는 EHR 정보 인프라에 초점을 두어 조직 전체의 정보보호관리를 다루고 있지 못하며 보안 기능과 정보관리 기능에 중복이 있어 관리지표로는 적합하지 않다.

4. 보건의료정보 보호관리 모델 개발

선행연구의 한계점을 보완하고 보건의료정보 보호관리 프로세스의 이행과 평가에 지침이 되는 프로세스별 세부 지표를 개발하였다. 국내 보건의료기관의 정보화 및 정보보호 관리 현황에 대한 이해를 바탕으로 BS7799, HIPAA 보안 규정, 그리고 HL7

EHR SIG의 EHR 기능 명세 등을 참고하여 국내 보건의료 환경에 적합한 정보보호관리 모델을 다음과 같이 제안하였다. 본 연구에서 제안하는 보건의료정보 보호관리체계는 10개의 프로세스, 25개의 이행 항목, 그리고 111개의 이행 지침으로 구성되어 있다. 다음은 이행 지침을 제외한 체계를 나타낸 것이다.

<표 1> 보건의료정보 보호관리 체계

정보보호 대책		이행 항목
1.0 준비/계획	1.1 정보보호 필요성 인식	1.1.1 정보보호 의지
		1.1.2 정보보호 투자
	1.2 정보보호 목적/전략분석	1.2.1 정보보호 목적 수립
		1.2.2 정보보호 전략 수립
2.0 현황분석/설계	2.1 위험분석/평가	2.1.1 조직 환경분석
		2.1.2 자산분석
		2.1.3 위험분석
		2.1.4 위험평가
	2.2 정보보호 관리 정책 수립	2.2.1 정보보호정책
		2.2.2 정보보호관리 담당자 지정
	2.3 정보보호 관리 프레임워크 설계	2.3.1 프레임워크 설계
		2.3.2 대상 솔루션 선정
		2.3.3 마스터플랜 수립
3.0 구현	3.1 관리적 보안	3.1.1 인적보안
		3.1.2 정보접근관리
		3.1.3 정보보호훈련/교육
		3.1.4 업무연속성 계획
	3.2 물리적 보안	3.2.1 매체보안
		3.2.2 설비보안
	3.3 기술적 보안	3.3.1 접근통제
		3.3.2 감사통제
		3.3.3 네트워크보안
		3.3.4 암호화
4.0 평가/유지	4.1 평가	4.1.1 준수 검토
	4.2 유지 관리	4.2.1 보안 사고대응

정보보호관리 방법론으로 위험에 따른 통제 관점의 접근이 대부분이었으나 이는 지속적인 개선을 위한 활동이 도출되지 못하는 한계가 있어 정보보호 프로세스의 관점에서 성숙도의 개념을 도입한 새로운 정보보호관리 방법론이 등장하고 있다.[12] IDEAL 모델, SDLC 방법론, BS7799, GMITS 정보보호 관리 프로세스를 참고하고 보건의료 환경을 고려하여 준비 및 계획, 분석 및 설계, 구현, 그리고 평가 및 유지의 4단계의 프로세스를 제시하였다. 상위 프로세스는 하위 프로세스를 가지며 각 단계의 산출물은 다음 단계에 연계되어 해당 프로세스의 자원으로 사용된다.

본 모델의 보호관리 대상은 보건의료기관이 생산, 처리, 관리하는 개인에 관한 모든 정보이며 이를 보건의료정보로 정의한다. 본 표준의 적용 대상은 보건의료정보를 취급하는 모든 보건의료기관으로서 보건의료서비스 제공기관, 보험기관, 위탁기관, 연구기관, 보건의료정보 관련 사업자, 공공기관 등이 포함된다. 적용 환경으로는 전산시스템의 부분적 활용 단계부터 모바일 기기, 칩, 무선 네트워크 시스템이 구축된 유비쿼터스 헬스케어 단계까지 모든 정보화 환경에 적용 가능하다.

5. 결론

본 연구에서는 보건의료 부문의 정보화 및 정보보호 현황을 파악하고 보건의료 부문의 특성을 분석하여 정보화의 편익과 함께 공존하는 역기능을 효과적으로 관리하기 위한 대책으로 보건의료 환경에 적합한 정보보호관리 모델을 제시하였다. 본 모델의 접근 방법은 보건의료정보시스템의 민감성, 집중성, 신속성, 연계성, 유연성, 확장성을 반영하여 조직이 요구하는 정보보호관리 행위를 효과적으로 정의·관리하며 지속적인 수준향상을 지원하는 프로세스 중심 설계를 채택하였으며, 통제항목 정리에 있어 높은 수준의 평가 기준을 제시하는 BS7799를 기반으로 보건의료정보의 관리에 대한 미국의 법령인 HIPAA 보안 규정과 보건의료정보의 전송 표준 규약인 HL7이 제시하는 EHR 기능 명세 중 정보보안과 관리 표준 등을 참고하였다. 보건의료 종사자의 행위적 특성을 고려하여 통제항목을 최소화하는 대신 컴퓨터 활용능력이 낮은 보건의료 종사자도 순서에 따라 쉽게 적용할 수 있도록 프로세스별 상세한 실행지침을 개발하였다.

국가 핵심 사업의 하나인 보건의료 부문 정보화 촉진 사업은 보건의료기관의 정보화를 지원하는 다양한 정책을 수행함으로써 보건의료 정보화 수준을 향상시키고 있다. 그러나 각 기관 간 상이한 정보화 구축 목표, 이해 당사자 간 합의 부족, 보안에 대한 국민적 우려, 표준 부재, 법제도 미비 등의 문제로 이미 구축된 정보시스템의 활용도가 기대에 미치지 못하는 실정이다. 선행연구 결과 정보제공자와 취급

자를 비롯한 보건의료정보시스템에 관련된 모든 사람들이 보건의료정보화에 있어 개인정보 유출과 보안 문제를 가장 큰 과제로 인식하고 있음을 알 수 있었다. 그럼에도 불구하고 요주의 정보인 보건의료정보를 보호하기 위한 노력은 극히 미미한 수준이다. 보건의료정보는 개인의 가장 민감한 정보로 최상의 보호가 이뤄져야하는 한편 국민 건강과 복지 향상을 위한 공익의 성격도 강하여 관리와 책임에 대한 명확한 지침이 더욱 필요하다. 보건의료기관의 정보보호관리 모델은 정보보호시스템 구축에 적정 투자 수준을 산정하고, 효율적인 관리 계획을 위한 통제 도구를 제공한다. 이러한 작업은 정보의 생성 단계부터 반영되어야 하므로 정보시스템의 설계·구축 시부터 보건의료정보 보호관리 계획이 포함돼야 한다.

참고문헌

[1] 김곤희, “우리나라 지역보건의료 EHR체계 구축 방안 연구”, 연세대학교 보건대학원 보건정보관리학과 석사학위논문, 2005.

[2] 김옥남, “진료정보의 등록 및 조사사업에서의 효율적인 자료 수집과 개인정보 보호 방안”, 대한의무기록협회 추계학술대회 논문집, pp. 32-35, 2003.

[3] 보건복지부, “2005년도 보건복지정보화촉진시행계획(안)”, 보건복지부, 2004.

[4] 임수연, “진료정보 공동활용에 대한 의사들의 참여의사 및 필요성 인식도에 관한 연구”, 연세대학교 보건대학원 보건정보관리학과 석사학위논문, 2004.

[5] 정혜정, 이경환, 김남현, “보건의료정보의 이용과 보호에 관한 법적 쟁점 고찰: HIPAA의 이해를 바탕으로”, 한국정보보호학회 동계학술대회 논문집, 14(2): pp. 462-466, , 2004.

[6] 정혜정, 김남현, “U-Healthcare 서비스 이용의도에 영향을 미치는 요인 연구”, 대한의료정보학회지, 11(1): pp. 46-47. , 2005.

[7] BSI, "BS7799", BSI, 1999.

[8] Candace Gray, “Understanding and Complying with HIPAA”, Journal of PeriAnesthesia Nursing, 18(3): pp. 182-185, 2003.

[9] HL7 EHR SIG, “HL7 EHR SIG Functional Descriptors”, HL7, 2003.

[10] Joseph Goedert, “Security: The Next HIPAA Rule to Tackle”, Health Data Management, 11(10): p. 14, 2003.

[11] Kevin Beaver and Rebecca Herold, “The Practical Guide to HIPAA Privacy and Security Compliance”, CRC Press LLC, 2003.

[12] M. M. Eloff and S. H. von Solms, “Information Security Management: An Approach to Combine Process Certification and Product Evaluation”, Computer and Security, 19, pp. 698-709, 2000.

[13] Margret Amatayakul, Steven S. Lazarus, Tom Walsh, “HIPAA Compliance: Have you completed a risk analysis?”, Healthcare Financial Management, 57(5): p. 96, 2003.

[14] NIST, “Security Self Assessment Guide for Information Technology Systems”, NIST Special Publication, 800-26, 2001.

[15] Pam Michael and Ellen Pritchett, “The impact of HIPAA electronic transmissions and health information privacy standards”, Journal of the American Dietetic Association, 101(5): pp. 524-528, 2001.

[16] SSE-CMM Project Team, “Systems Security Engineering Capability Maturity Model”, SSE-CMM, 1999.

[17] T.William Olle, et al., “Information Systems Methodologies (A Framework for Understanding)”, Addison-Wesley Publishing Company, 1991.

[18] U.S. Department Health and Human Services, “45 CFR Parts 160 and 164 Standards for Privacy of Individually Identifiable Health Information; Final Rule”, Federal Register, 67(157): Aug. 14, 2002

[19] U.S. HHS, “Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule”, NIH Publication, no. 03-5388, 2003.

[20] U.S. HHS, “Summary of the HIPAA Security Rule”, Office for Civil Rights, 2003.