의료정보화 및 보안 기술 표준화 동향

Technical Standards Trend of Health Informatics and Its Security

김신효 (S.H. Kim) 의료정보보호연구팀 선임연구원
송지은 (J.E. Song) 의료정보보호연구팀 연구원
정명애 (M.A. Chung) 의료정보보호연구팀 팀장
정교일 (K.I. Chung) 정보보호기반그룹 그룹장

목 차

최근 IT, BT, NT 등의 융합과 각 분야에서의 혁신적인 기술 발전은 건강하고 윤택한 삶에 대한 욕구와 부합하면서 의료 서비스 분야에서도 의료 장비 및 의료정보시스템, 의료 비즈니스 애플리케이션 등 관련 기술이 더욱 다양화되고 고도화되는 양상을 띄게 되었다. 그러나, 기술 대부분이 국가간, 심지어 동일 국가, 지역 내에서도 서로 다른 의료 기관이나 관련 업체간 긴밀한 상호 작용 없이 산발적, 독립적으로 개발이 수행되고 있어 통합 및 호환에 큰 어려움을 겪어 왔다. 이를 해결하기 위해 국내외적으로 의료정보 기술에 대한 표준화 움직임이 활발하게 이루어지고 있다. 본 고에서는 의료정보 기술의 개념 및 기술 개발 현황과 국내외 관련 표준 기술 동향을 살펴본다. 특히, 최근 의료 데이터 보안 및 프라이버시 보호의 중요성이 인식됨에 따라 이슈화되고 있는 의료정보보호 표준화 기술에 대해 보다 상세히 살펴본다.

Ⅰ. 서론

IDC의 2006년 IT 세계 시장 전망 자료에 의하면 향후 5년간 가장 높은 성장률을 보일 IT 분야로 통신/미디어와 함께 헬스케어가 선정되었다[1]. 단순히 병원 전산 정보 통합 수준이었던 의료정보화가 의료기기간 혹은 의료기관간 상호 호환을 중시하고 의료정보의 접근성 및 공유성을 확대시키는 유비쿼터스 헬스케어(이하 u-헬스케어) 서비스 형태로 진화하고 있는 것은 세계적인 추세이다.

u-헬스케어 서비스를 실현하기 위한 요소기술로는 바이오 칩 혹은 센서를 포함한 스마트 의료 디바이스와 이를 이용한 데이터 수집 기술, 수집된 의무 데이터의 표기 기술, 메시징 및 의료데이터 교환 기술, 의료정보 데이터 관리 및 가공서비스를 위한 정보 서버 기술, 안전한 의료 서비스 제공 및 프라이버시 보호를 위한 의료정보보호 기술 등이 있다. 이 외에도 의료 전문 용어의 정의, 의료전자카드 기술, 전자 투약 처방 및 전달 기술도 의료정보화 기술과 통합 연동되어야 한다. 하지만 이와 같은 기술들은 국가간 혹은 국가 내 의료 서비스 기관 및 관련 업체간에 협력과 긴밀한 상호 협의 없이, 산발적이고 독립적으로 개발되어 호환에 있어 한계에 부딪혀 왔다. 이를 개선하기 위하여 캐나다, 미국 및 유럽 등에서는 상호 호환 가능한 의료정보서비스를 보장하기 위해 국내 표준 및 법제, 기술 권고안 등을 제정해왔으며, CEN, ISO, IEEE, DICOM, HL7, IHE 등에서도 활발히 국가간, 기관간 의료정보 교류 및 공유, 시스템 통합 등을 염두에 둔 국제 표준을 활발히 개발중에 있다. 국내에서도 최근, 보건복지부 및 국내 산업표준위원회를 중심으로 전자건강기록(이하 EHR) 표준 및 관련 법안 마련 등에 박차를 가하고 있다.

● 용 어 해 설 ●

HL7 (Health Level 7): 서로 다른 의료 분야 소프트웨어간 정보 호환이 가능하도록 하는 표준 제정을 위해 1987년에 조직된 국제 표준화 기구를 의미하거나, 이 표준화 기구에서 마련한 의료정보 전송 표준 자체를 의미하기도 한다.

본 고에서는 의료정보화 기술 및 서비스 동향과 국내외 의료정보 기술 표준과 관련 법제 동향 등에 대해 살펴보고 최근 이슈화되고 있는 의료 데이터 보안, 프라이버시 보호에 관련한 의료정보보호 표준화 및 기술 동향을 보다 상세히 살펴본다.

Ⅱ. 의료정보화 기술 동향

의료서비스의 질을 향상시키기 위한 노력으로 의료정보화 사업이 활발히 추진되어 왔으며, 현재로서는 의료 서비스 혹은 헬스케어 시장에서 의료정보의 전산화 및 전산 통합 수준의 의료정보화가 대형 병원을 중심으로 활발히 이루어지고 있다. 의료정보화는 의료영상정보시스템(이하 PACS), 처방전달시스템(OCS)과 전자의무기록(이하 EMR)을 연동함으로써, 비용절감 효과 이외에 진료의 안정성 및 서비스 질 향상, 환자 대기시간 절감, 정보 저장의 편의성, 환자 기록에 대한 의료진의 접근성이 용이해질 것이다. 주요 의료기기 업체인 지멘스와 GE 헬스케어 회사도 진단 위주의 의료기기 뿐만 아니라 EMR, PACS, OCS 등의 통합 의료정보화 솔루션을 출시하고 있다[2],[3]. 아직까지 우리나라의 경우 원무 중심의 의료정보화가 이루어지고 있으며 EMR 도입은 저조한 편이다[4].

지금까지 병·의원에서 독자적인 형태로 관리되었던 EMR은 최근 개인의 평생 전자 건강 기록인 EHR의 개념으로 발전하게 되었다. 의무 기록의 전산 통합 수준이 아닌, 병원간 전자 기록 및 처방 정보의 공유, 환자 자신의 의무 데이터 소유 및 관리에 대한 욕구 반영, 양질의 의료 서비스를 위한 EHR 및 EHRS의 지능화가 요구된다. 이러한 EHR은 사용자 중심의 u-헬스케어 서비스를 위해서 선행되어야 할 가장 기본적인 서비스이며, 국가적 차원으로 국가보건 의료정보 인프라(NHII) 구축에 필수적이므로 이에 대한 기술 표준화 및 상용 수준의 시스템 개발이 지속적으로 확대될 것으로 전망된다. 또한, 현재 EHR 및 EHRS는 상호 운용성(interoperability) 및

접속성(connection)을 지원하기 위하여 의료기관간 데이터 공유, 관련 의학 용어 통일, 메시징 방식 및 인터페이스의 표준화가 진행되고 있다. 아울러 안전한 EHR 데이터의 보관 및 교환, 환자의 개인 프라이버시 보호 등 EHR 시장의 활성화를 가로막고 있는 보안 위협 요인들에 대한 이슈화 및 연구가 일부 이루어지고 있다[5],[6].

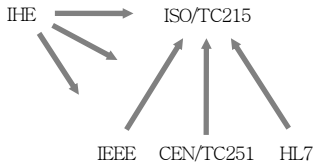
국가적으로 사용되기 위한 EHR 보안 및 프라이버시 보장을 위해서는 다음과 같은 방식의 문제 접근과 구체적 해결 방안이 제시되어야 할 것이다[7].

- 분산된 접근
- EHR 엔트리의 신뢰성
- 다른 목적으로 사용되는 EHR 정보 제한
- EHR 접근 프라이버시 보호
- 오프라인 EHR 접근 통제
- 의료정보에 대한 의료진 권한 보장
- 안전한 포터블 의료 건강 정보
- 사용자 인증
- 비침입적 EHR 공유

EHR 중심의 의료정보화 및 u-헬스케어 서비스 모델 등에 대한 활발한 연구가 수행되고 있으나, 보안 및 프라이버시와 관련된 연구는 아직까지는 미비한 실정이다. 이같은 보안 문제 측면에서 HIPPA의 의료정보 보안 및 프라이버시에 대한 논의는 큰 의미를 가진다. 이에 대한 자세한 내용은 제 IV장에서 다루기로 한다.

Ⅲ. 의료정보 기술 표준화 동향

의료정보 기술 표준의 범위는 의료 행위를 나타내는 용어 및 참조 모델, 진료 기록의 형식 및 서식, 정보의 메시징 방법 및 의료정보 보안과 같은 인프라 기술에서부터 의료 기기 규격 및 인터페이스 혹은 비즈니스 모델 요구사항 등에 이르기까지 다양하다. 또한, 의료정보 기술의 표준 이슈는 지역별 블록화 추세 강화, 적합성 및 상호운용성에 관한 관심의 증대, 지적재산권과 표준화간의 조화 문제, 표준 제정 과정에의 이용자 참여 증대 등과 같은 양상을 띄고 있다. 현재, 의료정보화와 관련된 대표적인 국제 표준 기구는 DICOM, IEEE, ISO 및 CEN, HL7, WHO와 SNOMED 등이 있다. 아울러, ITU에서는 의료정보의 무선 통신 규약에 관하여 UN/CEFACT와 OASIS에서는 의료 데이터 표기 및 메시징 기반 기술로서 XML, ebXML과 관련하여 활발히 논의중이다.



(그림 1) 표준화 기구간 상호 협력 관계

주요 표준화 기구간 상호 협력 및 연관 관계는 (그림 1)과 같다[8]. CEN/TC251과 HL7은 의료정보 및 통신에 관한 공동 표준 발굴 및 개발, ISO 표준 상정에 관한 양해각서를 체결한 상태이며 IEEE 또한 ISO와 함께 협의, 수립한 표준 워크플랜에 기초하여 제정한 표준에 대해 ISO 승인을 발행받는 형태로, 표준 기구간 중복 기술 개발 낭비 및 불일치 해소를 위한 협력 관계가 수립되어 있다.

1. HL7

HL7은 병원정보시스템 및 의료 장비 접속에 관한 표준을 제정하는 표준 기관으로서, 현재 한국을 포함한 29개국 지부를 두고 있으며 의료정보의 전자적 교환을 위한 ANSI 사실 표준(de facto standard)이다[9]. HL7은 ISO/OSI의 가장 상위레벨인 7계층의 응용을 의미하는 것으로서, 분산된 의료정보의 대용량 정보처리를 위하여 시스템간의 자료 전송을 최대한 효율적으로 수행하고, 전송중 발생하는 오류를 최소로 할 수 있는 표준의 정립을 목표로 하고 있다. 현재 개발중인 표준으로는 보건 의료정보 메시징 표준(V2.x, V3)과 HL7 데이터 모델인 참조정보 모델(이하 RIM), 의사 결정과 지식 지원을 위한 의학 로직 구문(MLM)에 관한 표준(Arden Syntax), 온라인 상에서 임상 정보를 공유할 수 있도록

하는 XML 타입의 데이터 구조 모델을 제시하는 임상 데이터 구조(이하 CDA)와 사용자 관점에서의 이기종간 산재된 독립된 애플리케이션 및 개인 정보의 통합에 관한 표준(이하 CCOW) 등이 있다.

HL7 메시징 표준은 추상적 메시지 구조, 메시지 코딩 규칙, 메시지를 촉발하는 애플리케이션 이벤트인 트리거 이벤트에 관한 명세서를 기술하고 있으며 현재 V2.x를 거쳐 V3까지 제안되어 있다.

한편, HL7 CDA 릴리즈 2.0은 XML과 HL7 RIM, SNOMED, ICD 등과 같은 의학 용어 코드 표준 등을 사용하여 기계 및 휴먼 가독성을 높였으며 XML 지원 가능한 웹 브라우저나 무선 애플리케이션까지 그 지원 범위를 확대시켰다. 현재 CDA 릴리즈 2.0은 2005년 완성, ANSI 승인된 상태이다.

2. DICOM

DICOM은 의료 디지털 영상과 부수적인 의료 통합 정보의 전송을 위해 TCP/IP 위에서 동작하는 표준 영상 신호 프로토콜로서 NEMA/ACR 위원회에 의해 개발되었으며, 현재는 다음 16개 분야의 표준화 규격이 존재한다[10].

- Part 1 – Introduction and Overview
- Part 2 – Conformance
- Part 3 – Information Object Definitions
- Part 4 – Service Class Definitions
- Part 5 – Data Structures & Semantics
- Part 6 – Data Element Listing and Typing
- Part 7 – Message Exchange Protocol
- Part 8 – Network Support for Message Exchange
- Part 10 – Media Storage and File Format for Media Interchange
- Part 11 – Media Storage Application Profiles
- Part 12 – Media Formats and Physical Media for Media Interchange
- Part 14 – Grayscale Standard Display Function
- Part 15 – Security and System Management Profiles
- Part 16 – Content Mapping Resource
- Part 17 – Explanatory Information
- Part 18 – Web Access to DICOM Persistent Objects (WADO)

한편, DICOM은 네트워크를 통한 실시간 디지털 의료 영상 전송 및 조회를 지원하는 PACS의 표준 기술로서 인식되고 있으며 데이터베이스, OS, 프로그래밍 언어, 하드웨어 등 구현과 관련된 내용은 포함하고 있지 않다.

3. ASTM

ASTM은 미국에서 유통되는 거의 모든 제품 및 재료에 대한 용도 및 특성을 시험하고 제품의 품질을 규격화 함으로써 제품 생산자와 사용자가 손쉽게 이와 같은 재료를 사용할 수 있도록 인증을 다루는 표준 기구로서, 현재 E31 기술 위원회에서 헬스케어 관련 표준화를 주도하고 있다[11].

ASTM의 E31 Healthcare Informatics 기술 위원회는 특정 환자 정보나 지식을 포함한 의료정보 및 의사 결정에 사용될 시스템 구조 및 기능, 내용, 저장장치, 보안 및 기밀성 보장과 정보 전달 등에 관한 표준 개발을 주 목표로 하고 있으며, 아래와 같은 하위 기술위원회를 포함하고 있다. 그러나 실제적으로는 E31.15, E31.25, E31.35 및 E31.90 정도가 활발히 활동하고 있다.

- E31.01 Controlled Health Vocabularies for Healthcare Informatics
- E31.15 Healthcare Information Capture and Documentation
- E31.19 EHR Content and Structure
- E31.20 Security and Privacy
- E31.22 Health Information Transcription and Documentation
- E31.23 Modeling for Health Informatics
- E31.25 Healthcare Data Management, Secu-

rity, Confidentiality, and Privacy
- E31.28 Electronic Health Records
- E31.35 Healthcare Data Analysis
- E31.90 Executive

특히 ASTM은 상호 운용성을 위해서 E31.28 워킹그룹의 E2369-CCR 규격을 HL7의 EHR 기능규격, CDA, RIM 등의 관련 표준 규격과 하모나이즈(harmonize) 과정중이다. 또한 ASTM 표준화는 미국내 표준이며, 의료정보화를 위한 새로운 기술 규격의 개발보다는 기존의 IEEE, ISO, HL7, DICOM, IETF 등의 국제 표준화 규격을 준용하며, 의료서비스에 적용하기 위한 관점의 표준개발이 대부분이다.

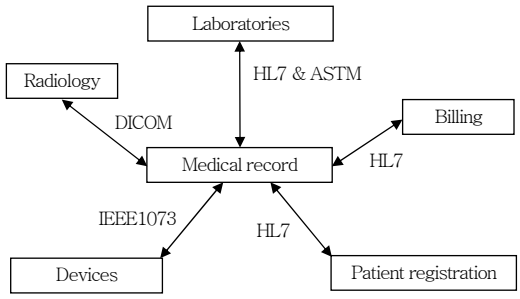
4. ISO/TC215

ISO/TC215는 의료장비간 데이터의 상호연계성 및 호환성 확보, 의료기록의 디지털화에 필요한 표준 개발을 목표로 하는 의료정보기술위원회이며, 다음과 같이 8개의 워킹그룹(WG)이 활발히 활동중이다[12]. 특히, WG4에서는 의료정보화 인프라 기술중의 하나인 보안 표준 기술을 정의하고 있으며 다음 장에서 보다 자세히 다루도록 한다.

- WG1: Data Structure
- WG2: Data Interchange
- WG3: Semantic Content
- WG4: Security
- WG5: Health Card
- WG6: Pharmacy and Medication Business
- WG7: Devices
- WG8: Business Requirements for EHRs

5. 표준간 상호 운용성

상호 운용성을 위한 표준 중에서 데이터 전송과 관련된 표준으로는 HL7과 DICOM이 있으며, EMR 콘텐츠에 대한 내용은 ASTM에서 정의되어 있다. 이들 표준들이 의료정보화에서 사용되는 상관관계는 앞서 설명한 (그림 2)에 도시하였다.



(그림 2) 의료정보 표준간 상호관계

IEEE1073은 의료기기간 실시간 플러그-앤-플레이 방식의 상호 운용성 제공을 목적으로, 이종 의료장비간 데이터 전송 및 공유가 가능하도록 하는 프레임워크와 전송 및 데이터 표준에 대한 논의를 진행하였으며, 현재는 ISO/TC215의 WG7과 통합되어 ISO/IEEE1073 작업이 진행중이다[13].

위와 같이 의료정보 전송 표준은 마련되어 있으나, 표준이 가지는 선택사항에 대한 구현 및 해석의 차이로 상호 호환이 원활하지 못한 것이 현실이다. 이러한 표준간의 조화와 구현 가이드 및 상호 운용성 보장을 위한 표준 적합성의 재해석 등을 수행하기 위해 IHE가 구성되었다. IHE는 HIMSS와 RSNA가 공동으로 추진한 의료정보 표준화 실현을 위한 일종의 촉진 기구로, 세계적으로는 100여 개의 벤더들이 참여하고 있다[14]. 현재 이 기구는 기존의 산업 표준들을 준수하여 의료정보시스템과 의료 영상기기 사이에 의료정보를 공유할 수 있도록 지원하는 5개의 프레임워크 및 37개의 통합 프로파일, 테스팅 및 데모 시나리오 등을 지원한다.

상호 운용을 위한 표준화 논의는 의료 종사자와 IT 서비스제공자 및 정부가 함께 해결해 나가야 할 최우선 선결 과제라고 할 수 있다. 하지만 현실적으로는 상호 운용성 제공 의료기관에 대한 경제적, 정책적 지원정책의 미비와 참여자인 의료인과 환자에 대한 적극적인 유도 정책 부재로 아직까지는 표준화가 미미한 형편이다. 따라서, 향후 예상되는 u-헬스케어 기술의 발전 추이에 따라 사용자 니즈 및 상호 운용성을 반영하여 보다 집중적인 표준화 제정 및 보급을 위한 노력이 수행되어야 한다.

Ⅳ. 의료정보보호 기술 표준

의료정보 기술 표준은 Ⅲ장에서 살펴본 바와 같이 ISO/TC215, ASTM, HL7, DICOM 등과 같은 표준화 기구들의 활동을 통해 독자적, 상호 협력적으로 개발되고 있다. 이러한 표준화의 노력으로 의료정보의 전송 및 공유가 진행될수록, 보안상 취약점에 노출되기 쉽고 결과적으로 안전한 의료 서비스가 위협 받을 수 있다. 따라서 최근 보안 기술은 의료정보화 표준 기술 영역에 필수불가결한 기술로 인식되고 있으며, 일례로 ISO/TC215에서는 WG4의 보안 기술을 의료정보화를 위한 4대 인프라 기술로 선정하였다. 본 장에서는 의료정보보호 기술 표준을 위한 각 표준화 기구의 표준 내용을 보다 상세히 기술한다.

1. ASTM E31.20

ASTM E31.20 보안 및 프라이버시 기술위원회에서 제정된 주요 표준은 아래와 같으며, 이들은 대부분 ANSI 표준으로 제정하기 위한 승인절차를 마친 상태이다.

- E1714-00, Standard Guide for Properties of a Universal Healthcare Identifier (UHID): 환자에 대한 유일한 식별성을 제공하며 동일한 환자에 대해서 다양한 형태로 연결 가능한 평생건강기록 파일을 생성할 수 있어야 하고, 의료정보보호를 위한 보안 기술이 적용되어야 하는 UHID 속성에 대해 언급하고 있다.
- E1762-95 (2003), Standard Guide for Electronic Authentication of Health Care Information: 디지털 서명 과정의 특성 및 속성과 메커니즘의 최소 요구사항을 정의하고 있으며, 의료서비스에서 활용 가능한 서명 기술을 기술하고 있다.
- E1869-04, Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Electronic Health Records: 이 표준은 기밀성, 프라이버시, 접근 그리고 개인을 식별할 수 있는 의료정보의 보안을 위한 원칙들을 언급하고 있다.
- E1985-98 (2005), Standard Guide for User Authentication and Authorization: 의료정보시스템을 사용하는 사용자(관리 또는 임상)를 인증하고 의료정보 문서의 접근이나 특정 작업을 허용하도록 하는 권한제어 메커니즘에 대한 내용이다.
- E1986-98 (2005), Standard Guide for Information Access Privileges to Health Information: 건강정보와 관련된 환자 및 제공자의 개개의 권리에 대한 내용이 포함되어 있다.
- E1987-98, Standard Guide for Individual Rights Regarding Health Information: 의료정보와 관련된 모든 개인(환자 및 공급자 포함)에 대한 권리와 권리 운영 절차에 대해 기술하였다.
- E2084-00, Standard Specification for Authentication of Healthcare Information Using Digital Signature: 서명 및 해시 알고리듬, 공개키/비밀키의 관리, 암호키 및 인증서의 형식, 의료정보 문서에 대한 서명 방법 등이 주요 내용이다.
- E2085-00a, Standard Guide on Security Framework for Healthcare Information: 이 표준은 의료정보를 위한 새로운 표준의 제안보다는 상호 운용성을 지원하는 프로토콜과 메시지 형식을 기존 표준을 재사용하거나 확장하여 사용하도록 정의한다.
- E2086-00, Standard Guide for Internet and Intranet Healthcare Security: 인터넷 프로토콜을 사용하는 네트워크에서의 의료정보를 안전하게 보호하기 위한 메커니즘에 대해 기술하고 있다.

2. ISO/TC215 WG4

ISO/TC215는 의료정보보호와 관련된 사항을 WG4에서 진행중이며 표준화 내용은 다음과 같다.

- ISO/DIS 17090-1: Health informatics - Public Key Infrastructure—Part 1: Framework and overview: 헬스케어 환경의 PKI에 대한 기본 정의와 컴포넌트를 정의하고 상호 호환성 보장을 위한 요구사항, 보안 서비스 시나리오, PKI에서 사용되는 인증서 종류 및 공개키 암호 기술 등을 기술하고 있다.
- ISO/DIS 17090-2: Health informatics - Public Key Infrastructure—Part 2: Certificate profile: 의료정보시스템 환경의 특성을 반영한 PKI 인증서 프로파일 명세서이다.
- ISO/DIS 17090-3: Health informatics - Public Key Infrastructure—Part 3: Policy management of certification authority: 헬스케어 PKI 구축 및 운영을 가이드 라인으로서, 인증서 정책의 구조 및 요구사항, 인증서 정책의 구조, 요구되는 보안 레벨, 보안 정책 내에 포함되어야 할 요구사항 등을 기술하고 있다.
- ISO/DIS 27799: Security Management in Health using ISO/IEC 17799: 의료정보시스템 환경에서 요구되는 전반적인 보안 기술에 대한 가이드라인과 같은 표준 문서로서 보안의 목표, 보안 대상 자원, 발생 가능한 공격 및 취약점, 요구되는 보안 기술 등을 포함하고 있다.
- ISO/TS 22600-1: Health informatics - Privilege management and access control—Part 1: Overview and policy management: 다자간 의료정보의 전달 및 공유가 이루어지는 환경에서 정보에 관한 권한관리 및 접근 제어 방법을 제시한 기술 표준으로서, 관리 대상 데이터 분석, 권한 정책 항목 분석, 권한 관리 시나리오 등을 주로 기술하고 있다.
- ISO/TS 22600-2: Health informatics - Privilege management and access control—Part 2: Formal models: 의료정보 권한 관리 모델(도메인 모델, 정책 모델, 역할 모델, 위임 모델, 접근 제어 모델 등)을 제시하고 있다.

현재, Health informatics - Classification of safety risks from health software (ISO/DTS 25238) 표준은 진행 여부에 대한 투표가 진행중이며, 이외에 추적 감사, 파일 보관 및 익명화(pseudonymisation)에 대한 표준화 필요성이 제기된 상태이다.

3. HL7 SIG

HL7은 보안 특별 관심그룹(SIG)을 통해서 HL7 메시지가 라우터 중계로 통신하는 경우 발생 가능한 보안 위협을 하위 네트워크, 종단간 네트워크, 세션 중심 응용, 저장 및 전달 중심 응용 등 통신 계층에 따른 위협으로 분류하였다. 또한, 이들 각각에 대하여 인증, 권한 관리와 접근제어, 무결성 및 기밀성 보장, 부인방지 등 보안서비스 요구사항을 정리하였다[15]. 현재 HL7 보안 기술위원회는 보안 서비스 프레임워크(HL7 Security Service Framework)와 HL7 EDI 통신보안에 관한 가이드(Standard Guide for Implementing HL7 EDI Communication Security) 작성의 필요성이 인식되고 있어 앞으로도 표준화 작업을 활발히 진행할 것으로 기대된다.

4. 의료정보보호 법·제도

의료정보보호 표준화는 위와 같은 기술적인 내용 이외에도 법·제도와 관련된 내용이 더 활발하게 이루어지고 있으며, 대표적으로는 미국의 건강보험 이전가능성 및 책임에 관한 법률(이하 HIPPA)이 있다. 이 법률에서 개인 프라이버시와 보안을 포함하는 개인의료정보보호에 대한 언급을 하고 있다. 또한 보호되어야 할 개인 건강의무기록(Protected Health Information)이라는 의미로 PHI로 명명하였으며, 개인 신원 확인 정보(이름, 사진, 주소, 주민번호 등 개인을 식별할 수 있는 모든 정보)와 의료기록, 치료비, 과거/현재/미래 병력 등이 이에 해당한다.

HIPPA 프라이버시 규칙이 가지는 의미는 특히 환자 개인에 대하여 개인건강기록 공개제한 요구 권리, 비밀연락과 건강 기록수정 요청 권리, 공개 내역에 대한 권리, 개인 건강 기록 조사 및 사본 입수 권리 및 침해 발생시 진정서를 제출할 수 있음을 명시

하고, 환자의 허가나 동의가 필요한 경우를 분명히 정의함으로써 의료정보의 제공시 프라이버시 침해를 최소화하고 법적 분쟁 소지를 없애는 효과를 주었다는 점이다.

또한 HIPPA의 보안 규칙에서는 관리상의 안전장치(administrative safeguard), 물리적인 안전장치(physical safeguard), 기술적인 안전장치(technical safeguard)를 정의하고 있다[16]. 관리적 측면의 안전 장치는 보안 관리 절차, 정보 접근에 대한 관리 노동인구에 대한 보안, 보안 인지 및 훈련, 보안 사고의 처리, 긴급사태에 대한 대책과 평가 등이 있다. 물리적인 측면의 안전장치로는 설비에 대한 접근제어, 워크스테이션의 사용과 보안, 디바이스 및 미디어에 대한 제어를 포함한다. 기술적인 측면의 안전장치로는 접근제어, 감사 통제(audit control), 무결성, 접근자 및 엔티티에 대한 인증과 전송 보안이 있으며, 이에 대한 구현 요구사항은 <표 1>과 같다.

기술적인 안전장치의 구현 요구사항에 따르면, 유일무이한 식별자(ID)로 ePHI에 접근하여야 하고 비상 시에도 접근 가능한 절차가 있어야 하며, 저장 정보의 접근 및 변경에 대한 추적성 제공을 위한 감사 통제와 접근자 및 엔티티에 대한 인증은 반드시 제공되어야 하는 구현 규격으로 제시되고 있다. 표에 도시되어 있지는 않지만, 데이터 저장 및 전송 시의 암/복호화와 인증 기능, 그리고 PHI에 대한 위·변조 방지를 위한 무결성 제어는 보안에서 가장 중요한 고위험으로 분류할 수 있을 것이다[17].

〈표 1〉 HIPPA 보안규칙의 기술적인 안전장치

Technical Safeguard		
Standards	Implementation Specifications (R)=Required, (A)=Addressable	
Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Control		R
Integrity	Mechanism to Authenticate Electronic Protected Health Information	A
Person or Entity Authentication		R
Transmission Security	Integrity Controls	A
	Encryption	A

그러나 HIPPA가 의료정보 프라이버시와 보안에 대해서 언급하고 있으나, 데이터의 소유권에 대해서는 언급하지 않아 진료자료의 소유권 문제가 발생할 소지가 있는 것이 사실이다. 즉, 휴·폐업으로 인한 해당 기관의 개인의료정보는 누구에게 귀속되어 관리되어져야 하는지에 대한 명확한 규정이 정립되어 있지 않고 프라이버시는 개인에 따라 매우 다르게 규정될 수 있는 사항이다. 따라서 국내 의료 관련 정보보호 법·제도 제정 및 보완 시에 의료 데이터의 보안 및 프라이버시뿐 아니라 소유권에 관한 문제도 반드시 심각하게 고려해야 한다.

이 외에, 의료정보보호 관련 인증 기준으로서 CCHIT가 제정한 EHR 보안 기준이 있다. 미국 정부가 건강 정보 기술(이하 HIT)의 광범위한 사용과 EHR의 일상적 사용을 촉구하면서, 미 HIT 산업협회는 HIT 제품을 인증하기 위한 자발적인 민간 조직으로서 CCHIT를 설립하였다. CCHIT는 기능, 상호연동, 보안과 신뢰성, 인증 프로세스 등 4개의 WG을 운영하고 있고 보안 WG의 경우, 외래 환자용 EHR 보안 기준과 입원 환자용 EHR 보안 기준을 개발하고 있다. CCHIT가 제정한 외래 환자용 EHR 2006년 보안 기준의 경우, 접근 통제, 보안 감사, 인증, 보안 기술 서비스, 백업/복구, 보안 기술 문서 제공 등의 내용을 골자로 하고 있다[18].

국내의 경우 개인 의료정보보호, 원격 의료 시설, 전자 의무 기록 등과 관련, 처방 및 의료정보 등의 환자 비밀 준수 조항, 전자 의무 기록 관리 및 보관

● 용 어 해 설 ●

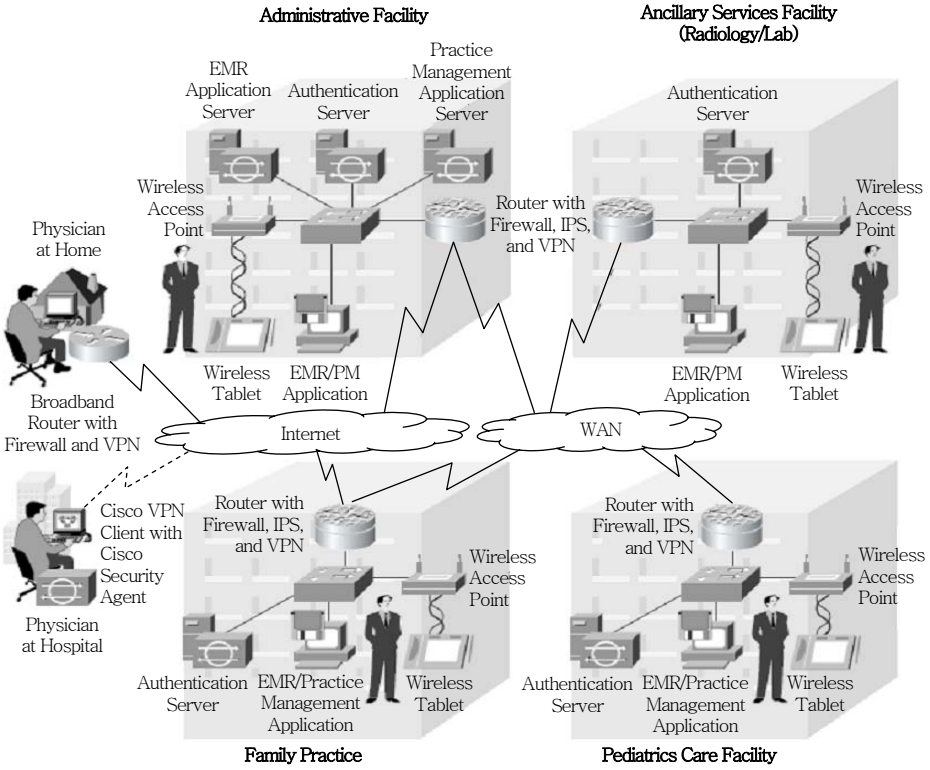
EHR (Electronic Health Record): 개인의 병원 관련 이력들이 저장된 전자의무기록(EMR)에서 발전하여 개인의 건강과 관련된 모든 정보를 포함하는 평생전자건강기록을 의미하며, 의료기관간, 의료정보시스템간 정보공유를 가능하게 한다.

의무화 등과 같은 현행 의료법 조항을 규정하고 있으며, 2006년 보건복지부는 보건 의료정보화 사업 추진과 관련하여 건강 정보보호 체계를 구축하기 위해 환자의 개인 의료정보보호 및 프라이버시 보호 권리, 개인 의료정보 취급자의 보호조치 의무와 책임, 의료정보 관리 절차 등을 포함한 개인의료정보보호법 제정을 위해 건강정보보호자문위원회를 운영중이다.

V. 의료정보보호 기술 동향

의료정보보호 기술은 타 정보보호시스템 기술과 마찬가지로 독자적으로 존재하는 기술이 아니라 의료정보시스템(또는 의료기기 제품)에 보안기술이 내재된 형태로 운용되고 있다. 또한 TCP/IP 기반의 인터넷 프로토콜이 의료장비에 필수적으로 지원되면서, 기존의 네트워크 장비 회사는 네트워크 정보보호 솔루션을 의료분야 정보보호에 그대로 사용할 수 있을 것으로 판단하고 있다. 즉, 헬스케어 네트워크에 대한 보안 장비는 네트워크 장비(스위치나 라우터 등) 내장용 바이러스 백신, 침입탐지, VPN 장비 및 보안 관리, 사용자 인증을 위한 AAA 장비, PoC 장비와 의료단말용 태블릿 PC 또는 PDA에 적용하기 위한 무선 보안 구간 인증 및 암호 툴 등으로 기존 보안 장비와 큰 차이가 없다. 이러한 헬스케어 네트워크 보안 구성 예시는 (그림 3)과 같다[19]. 하지만 이러한 구성은 네트워크 보안 관점에서의 구성일 뿐이며, 유비쿼터스 환경에서의 헬스케어 보안과 사용자 프라이버시에 대한 고려는 포함하고 있지 않다. 마찬가지로, 무선 네트워크 보안 문제는 PoC나 u-헬스케어 서비스에서 주로 사용될 무선 네트워크와 무선 단말에 대한 보안 이슈로 의료정보화와 관련된 특별한 이슈라고 보기는 어렵다.

반면, 개인프라이버시 보호에 대해 관심을 갖는

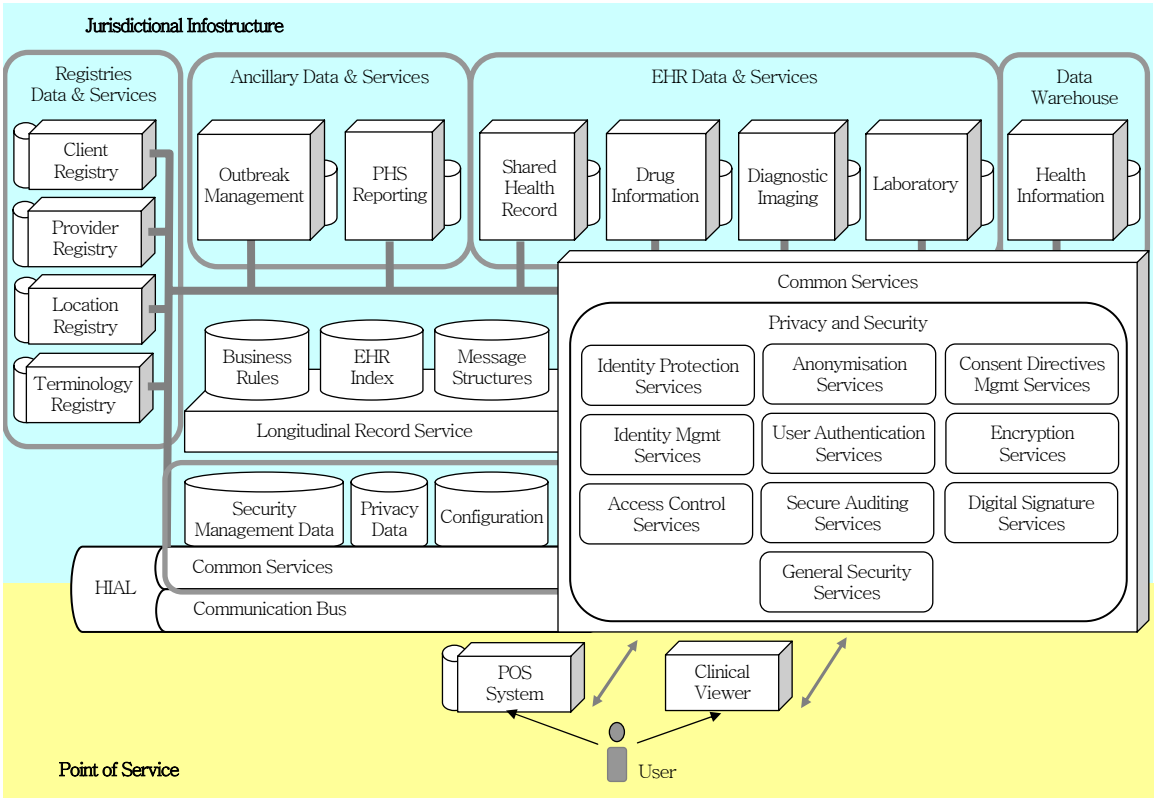


(그림 3) 시스코의 헬스케어 네트워크 보안 구성 예

사회적 분위기, 언제 어디서나 개인의료정보에 대한 접근과 수집이 가능해지는 u-헬스케어 서비스 등장으로 인해 개인 의료정보보호에 대한 우려의 목소리는 점차 커지고 있는 추세이다. 또한 의료정보가 통합되어 관리되는 경우, 데이터를 제공하는 주체인 환자와 데이터를 가공 및 사용하는 주체인 의료기관 종사자(의사, 간호사, 보험사 등)간 욕구 차이는 의료정보서비스의 공공성 및 편리성과 개인 의료정보 보호 권한 간의 상충을 초래할 수 있다[20]. 이는 의료서비스를 제공받는 환자 입장에서는 개인 의료정보에 대한 철저한 보호가 필요하지만, 치료 기법의 향상과 의료통계 및 임상연구에 의료정보를 활용하고 의료서비스를 선진화 함으로써 공공 이익에 기여하기 위해서는 개인 정보의 공유 및 활용이 반드시 요구되기 때문이다.

이러한 문제점을 해결하기 위해 캐나다는 Canada Health Infoway Inc.를 조직하고, EHR의 상호운용성 보장을 목표로 연구 개발을 진행하고 있다[21]. Health Infoway의 EHRS Blueprint Evolution 프로젝트는 여러 곳에 산재되어 있는 EHR 데이터를 통합하고 이들 간 상호 운용성을 보장하기 위해 HIAL, 즉 공통 통신 및 서비스 인터페이스 계층을 제공하는 EHR infostructure(즉, EHRi)를 정의하면서부터 시작되었다[22].

EHRi에서는 기본적으로 제공해야 할 공통 서비스로 데이터 서비스, 비즈니스 서비스, 메시징 서비스, 프로토콜 서비스, 상호 운용성 서비스, 가입서비스, 컨텍스트 서비스 및 일반 서비스 외에 중요한 항목의 하나로 보안과 프라이버시 서비스를 지정하고 있으며, PACA 프로젝트를 통해 보안 모델을 제안하고 있다. 이 프로젝트 그룹에서는 (그림 4)와 같은 보안 서비스 제공을 목표로 제시하였다. 아울러 (그림 4)는 EHRi 시스템 아키텍처, 서브 엔티티 간의 구성 관계 등을 도시하고 있다.



(그림 4) EHRi의 프라이버시와 보안 서비스

EHRi의 공통의 프라이버시 및 보안 서비스에는 사용자 식별자 관리 및 인증, 접근제어, 익명성 제공, 암호, 디지털 서명, 보안 감사 기록, 바이러스 탐지 등의 기본 보안 서비스 등을 포함한다. 의료정보화에서 필요한 보안과 프라이버시를 공통의 서비스로 정의하고 이를 위한 보안 프레임워크를 구성한 시도는 상당히 체계적인 접근이라 생각된다.

Ⅵ. 결론 및 시사점

이상적인 의료정보화 실현을 위해서는 의료 데이터의 공유 범위가 전체 의료기관에 걸쳐져야 한다. 그러나 의료정보의 특징은 정보 접근 및 활용의 긴급성을 요하면서도 환자 개인의 프라이버시가 철저하게 지켜져야 하는 양면성도 있다. 비표준화 시스템은 궁극적으로 의료서비스의 범위, 긴급성, 보안성 등 모든 면에서 불필요한 비용을 발생시킨다는 점에서 표준화의 중요성은 재차 강조해도 지나치지 않는다. 현재까지는 국내 의료정보시스템이 표준화 논의가 다소 미비한 채로 구축되는 현실이며, 이는 향후 국가 차원의 의료 경쟁력 향상에 부정적인 영향을 줄 것으로 염려되고 있다. 따라서, 편리성과 효율성, 상호 운용성이 보장되는 의료정보화 서비스의 실현을 위하여 표준화된 의료정보화 기술 개발이 필수적이다. 뿐만 아니라 안전한 의료 서비스 제공 및 사용자의 거부감 혹은 저항을 최소화하기 위해 의료정보 데이터의 보안 및 기밀유지, 프라이버시 보호 등을 위한 기술적, 법제도적, 윤리적 측면 등 다각적인 고려가 필요하다. 바이오 칩이나 센서, 무선 의료기기 등 보다 지능화된 의료장비들이 거미줄처럼 얽혀서 다양한 서비스 제공이 가능한 고도화된 u-헬스케어 서비스는 지금까지 언급된 의료정보보호 표준화와 정보보호의 완성으로 실현될 수 있을 것이다.

약 어 정 리

AAA	Authentication, Authorization and Accounting
ACR	American College of Radiology
ANSI	American National Standards Institute
ASTM	American Society for Testing and Material
CCHIT	Certification Commission for Healthcare Information Technology
CCOW	Clinical Context Object Working group
CCR	Continuity of Care Record
CDA	Clinical Document Architecture
CEN	Committee for European Normalisation
DICOM	Digital Imaging and Communication in Medicine
EHR	Electronic Health Record
EMR	Electronic Medical Record
ePHI	electronic PHI
HIAL	Health Information Access Layer
HIMSS	Health Information and Management Systems Society
HIPPA	Health Insurance Portability and Accountability Act
HIT	Health Information Technology
HL7	Health Level 7
ICD	International Classification of Diseases
IDC	International Data Corporation
IEEE	Institute of Electrical and Electronic Engineering
IHE	Integration of Healthcare Enterprise
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MLM	Medical Logic Module
NEMA	National Electrical Manufactures Association
NHII	National Healthcare Information Infrastructure
OASIS	Organization for the Advancement of Structured Information Standards
OCS	Order Communication System
PACA	Privacy and Security Conceptual Architecture
PACS	Picture Archiving Communication System
PHI	Protected Health Information
PoC	Point-of-Care
RIM	Reference Information Model
RSNA	Radiological Society of North America
SIG	Special Interest Group
SNOMED	Systematized Nomenclature of Medicine

UN/CEFACT UN/Center for Electronic FACT
WG Working Group
WHO World Health Organization

참 고 문 헌

[1] "IDC Expects Healthy Worldwide Investments in IT with Highest U.S. Growth Rates in Healthcare and Communications and Media," 2006, http://www.idc.com/getdoc.jsp?containerId=prUS20067406

[2] GE 헬스케어 홈페이지, http://www.gehealthcare.com

[3] 지멘스 메디컬 분야 홈페이지, http://www.medical.siemens.com

[4] 한국전산원, "의료정보화의 현황 및 과제," 2005, http://www.nca.or.kr/homepage/main/data/issue.nsf/9492337178066bdd49256dc800566e8a/ad87edcf8fb5eca2c9257022000faf2a/$FILE/_f8d4kukj5e1nn4t1d64oh3i53_.pdf

[5] J.S. Wimalasiri, P. Ray, and C.S. Wilson, "Maintaining Security in an Ontology Driven Multi-Agent System for Electronic Health Records," *Enterprise Networking and Computing in Healthcare Industry, 2004. HEALTHCOM 2004. Proc. 6th Int'l Workshop*, 28-29 June 2004.

[6] J.S. Wimalasiri, P. Ray, and C.S. Wilson, "Security of Electronic Health Records Based on Web Service," *Enterprise Networking and Computing in Healthcare Industry, 2005. HEALTHCOM 2005. Proc. of 7th Int'l Workshop*, 23-25 June 2005.

[7] Walt Culbertson, "Legal and Privacy Impacts of EHR and the National Health Information Network (NHIN)," 2005, http://www.sharpworkgroup.com/presentations/WEDI111705.pdf#search=%22Limiting%20Secondary%20use%20of%20EHR%22

[8] Y.S. Kwak, "Overview of Health Informatics Standardization," NI2004 Rio de Janeiro, June 2003.

[9] HL7 홈페이지, http://www.hl7.org

[10] DICOM 홈페이지, http://medical.nema.org

[11] ASTM E31기술위원회 홈페이지, http://www.astm.org/cgibin/SoftCart.exe/COMMIT/COMMITTEE/E31.htm? E+ mystore

[12] ISO/TC215 홈페이지, http://www.iso.org/iso/en/stddevelopment/tc/tclist/TechnicalCommitteeDetailPage.TechnicalCommitteeDetail?COMMID=4720

[13] IEEE 1073 홈페이지, http://www.ieee1073.org/standards/ 1073standards.html

[14] IHE 홈페이지, http://www.himss.org/ASP/topics_ihe.asp

[15] Kratz and Mary et al., "Health Level Seven Security Services Framework," 1998, http://www.hl7.org/library/committees/secure/HL7_Sec.html

[16] CMS, "HIPPA Security Series: Security Standards, Technical Safeguards," 2005, www.cms.hhs.gov/EducationMaterials/Downloads/SecurityStandardsTechnicalSafeguards.pdf

[17] "Summary of the HIPPA Privacy Rule," http://www.hhs.gov/ocr/hipaa/privrulepd.pdf

[18] "Final Criteria: Security and Reliability for 2006 Certification of Ambulatory EHRs," 2006, http://www.cchit.org/files/Ambulatory%20Domain/Final%20Criteria%20-%20SECURITY-RELIABILITY%20-%20Ambulatory%20EHRs%20-%202006.pdf

[19] Cisco Systems, Inc., "Medical-Grade Networks-Cisco Protected Healthcare Solutions for Physician Groups and Clinics," http://www.cisco.com/web/strategy/ docs/healthcare/physician_guide.pdf

[20] 박건희, "보건의료정보화와 개인정보보호," 서울대 의대 2006년 상반기 토픽 리뷰, 2006. 6.

[21] 캐나다 Health Infoway Inc. 홈페이지, http://www.infoway-inforoute.ca/en/home/home.aspx

[22] Canada Health Infoway Inc., Electronic Health Record Infostructure (EHRi) Privacy and Security Conceptual Architecture, Version 1.1, June 2005.