전자의무기록 보안표준화에 대한 고찰*

The Consideration about an Electronic Medical Record Security Standardization

박두희** · 송재영*** · 이남용****
Doo-Hee Park · Jae-Young Song · Nam-Yong Lee

차 례

1. 서 론
2. 관련연구
3. 개인의료정보 보호방안 수립
4. 전자의무기록 보안 표준화 수립
5. 결 론
• 참고문헌

초 록

인터넷의 발달로 개인정보의 수집 및 이용이 일상화됨에 따라 개인정보의 침해가 급속도로 확대되고 있다. 의료분야에 대한 개인정보보호에 대해서는 '정보통신망이용촉진 및 정보보호 등에 관한 법률' 등에 체계적으로 규정되어 있으나, 법적용 대상이 정보통신 서비스 제공자 위주로 규정되어 의료분야에 적용하는 데 한계가 있다. 때문에 본 논문에서는 국내 의료기관이 전자의무기록 시스템에 보안을 적용하기 위해 우선적으로 선행되어야 할 개인의료정보 보호방안에 대해 정의하고, 적용근거를 위한 법·제도의 검토사항을 제시하였다. 또한, 전자의무기록에 대한 전자서명의 구체적인 적용방안을 예시하여 의료분야에 있어서 보안적용을 위한 기준을 제시하였다.

키 워 드

의료, 개인정보보호, 전자의무기록, 보안, 개인의료정보, 전자서명

* 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌음
** 숭실대학교 대학원 컴퓨터학과 박사과정 수료, 보건복지부 정보화담당관실 사무관
(Ph. D. Program, Department of Computer Science, Soongsil University, Deputy Director, Ministry Of Health and Welfare, Information Management Division, dhpark@mohw.go.kr)
*** 숭실대학교 대학원 컴퓨터학과 박사과정 수료, 노동부 정보화추진단장
(Ph. D. Program, Department of Computer Science, Soongsil University, Director, Ministry Of Labor, Information Development Division, jysong@molab.go.kr)
**** 숭실대학교 컴퓨터학부 교수
(Professor, Department of Computer Science, Soongsil University, nylee@comp.ssu.ac.kr)
• 논문접수일자 : 2005년 2월 3일
• 게재확정일자 : 2005년 3월 8일

ABSTRACT

Due to the development of Internet and the collection and usage of the individual information, the infringements of the personal data have been increased rapidly. Regarding the personal data protection in the medical industry, it is clearly described in 'Act on Promotion of Information and Communication Network Utilization and information Protection, etc.'. the law is ratified on the basis of the service provider, therefore, it has its own limitation to be applied to medical industry. Therefore, this paper is to set the security standard and to discuss the range of legal application and considerations on its basis for the domestic medical institution at the electronic medical record system. We exemplify specific applicable content of the electronic signature in the electronic medical record also, present a security assessment item in electronic medical system and set the criteria for the security standard in the medical industry.

KEYWORDS

Medical, Personal data protection, Electronic medical record, Security, Personal medical data, Electronic signature

1. 서 론

전자의무기록은 전자적으로 수집, 관리, 사용, 전송되는 환자의 진료정보 뿐 아니라 환자의 인적사항 정보와 같은 개인정보와 직접적으로 연관되기 때문에 보안이 무엇보다도 중요하다. 따라서, 전자의무기록의 생성 · 보관 · 열람 · 유통 · 폐기 등 생명주기 각 단계마다 취해져야 할 보안표준 또는 지침이 보다 구체적으로 마련되어야 한다.

이를 위해 정부는 지난 2002년 3월, 의료법 제21조의 2 (전자의무기록) 및 2003년 10월 동법 시행규칙 제18조의 2(전자의무기록의 관리 · 보존에 필요한 장비) 등 전자의무기록의 법적 근거를 마련하였으며, 의료법 제19조(비밀누설의 금지), 20조(진료기록 등)의 조항에 의하여 개인 진료정보의 부적절한 유출을 금지하고 있으며, 동법 제21조의 2(전자의무기록)에 의하여 전자의무기록의 보호 및 정보유출 방지를 규정하고 있다. 또한, 개인정보의 보호를 위해 정부차원에서는 '공공기관의 개인정보보호에 관한 법률' 및 '정보통신망이용촉진 및 정보보호 등에 관한 법률' 시행령에 근거하여 수행하고 있으며, 민간부문에서는 '민간부문의 개인정보보호에 관한 법률'을 정보통신부가 입법예고하는 등 전자의무기록의 보급을 촉진시

키기 위해 적극적인 노력을 하고 있다.

그러나 국내 의료기관의 경우, 개별적으로 보안표준화를 추진하고 있어서 표준화에 대한 중복적인 노력이 소요되고 있을 뿐만 아니라, 각기 다른 보안표준설정에 따른 기술적인 문제의 발생이 예상되고 있다. 또한, 의료기관에서 운영되고 있는 전자의무기록 시스템에서는 사용자인증시 기본적으로 아이디와 암호를 사용하고 있으나, 이러한 아이디와 암호는 주기적인 갱신이 필요하고, 도난 · 분실의 경우에는 정보손실은 물론, 해커에 의해 정보내용이 위 · 변조되거나 개인의 진료정보가 유출될 우려가 크고, 사용자가 정보이용 사실을 부인할 경우 이를 명확하게 입증할 방법이 없다.따라서, 전자의무기록에 대한 전자서명의 구체적인 적용예시 및 지침을 통해 전자의무기록에서의 보안의 적용을 용이하게 하고, 보급을 촉진하여야 할 필요성이 요구된다.

따라서, 본 논문에서는 국내외 개인정보보호와 관련된 법 · 제도를 검토하여 전자의무기록에서 보안을 적용하기 위해 우선적으로 의료분야의 보안적용 범위를 '개인의료정보'로 규정하고, 개인의료정보에 대한 정의 및 범위를 설정하였다. 이를 통해 전자의무기록 관련 법률을 재해석하여 추가적인 검토사항을 도출하였다. 그리고, 전자의무기록에 대한 전자서명의 적용을 구체적으로 예시하였으며, 그 적용지침을 마련하였다. 이를 통해 국가차원에서 의료분야의 보안성강화를 위한 방향 및 기술적인 적용의 혼선을 방지할 수 있는 기준을 설정하였다.

2. 관련 연구

2.1 국내외 개인정보보호 관련 법 · 제도

2.1.1 공공기관의 개인정보보호에 관한 법률

국내 공공기관의 컴퓨터에 의하여 처리되는 개인정보는 그 취급에 관하여 필요한 사항을 정한 법률 제05715호에 의거하여 보호된다(한국. 공공기관의 개인정보보호에 관한 법률시행령, 대통령령 제18312호).

2.1.2 정보통신망 이용촉진 및 정보보호 등에 관한 법률

국내의 개인정보는 정보통신망 이용을 촉진하고, 정보통신 서비스를 이용하는 자를 보호하기 위한 법률 제7139호를 적용하여 보호된다(한국. 정보통신망 이용촉진 및 정보보호 등에 관한 법률시행령, 대통령령 제18505호).

2.1.3 HIPAA(The Health Insurance Portability and Accountability Act, 1996) Privacy Rule

미국은 1996년 제정된 Public Law 104 191(Kennedy Kasselbaum Act로도 불림)에 근원으로 HIPAA라는 법률을 제정하였다(HIPAA 2003). 이는 개인 및 단체 의료보험의 이전과 연속성을 개선할 목적으로 마련되었으나, 의료보험 관리절차의 간소화로 그 범위가 확대되고, 의료정보의 전자적 교환과 표준적용이 가능하게 되었다. 관리절차 간소화 부분에서

는 트랜잭션 및 코드 집합, 인적사항 식별, 보안(Security), 개인정보보호(Privacy), 기간, 벌금 등을 규정하였다.

개인정보보호(Privacy)와 관련하여 HIPAA는 part 164 subpart E(Standard for Privacy of Individually Identifiable Health Information)에서 관련 규정을 다루고 있다. 의무기록의 어떤 사용과 공개가 필요하고, 인가되는지 또는 자신의 의무기록에 대해 개인이 어떤 권리를 가지고 있는지를 설명함으로써 어떻게 의무기록이 통제되는지에 관한 규정을 정의하였다. 이 규정은 기존 의무기록 또는 전자문

〈표 1〉 국내외 개인정보보호 관련 법 · 제도

관련근거	개인정보보호 항목
공공기관의 개인정보보호에 관한 법률	개인정보의 수집, 개인정보 파일의 공고 개인정보 파일 대장의 작성, 개인정보의 안전성 확보 개인정보 취급자의 의무, 처리정보의 이용 및 제공의 제한 처리정보의 열람 및 제한, 열람의 결정 및 통지 처리정보의 정정, 정정의 결정 및 통지 대리청구, 수수료
정보통신망이용촉진 및 정보보호 등에 관한 법률	개인정보의 수집 및 제한, 개인정보의 이용 및 제공 개인정보 수집 등의 위탁, 개인정보 관리책임자의 지정 개인정보 취급자의 제한, 개인정보의 보호조치 및 파기 이용자의 권리 및 정보보호, 정보통신망의 안정성 확보 정보보호 안전진단, 정보보호관리체계의 인증 정보통신망 침해행위 등의 금지, 침해사고의 대응 국외이전 개인정보의 보호, 비밀유지, 벌칙
HIPAA Privacy Rule	치료, 지불, 의료 운영을 위한 사용과 공개 인증이 필요한 사용과 공개(정신치료기록, 마케팅 활용) 개개인의 찬성 · 반대가 필요한 사용과 공개(의무기록 사본 제공, 의료, 통지) 인증, 찬반이 필요 없는 사용과 공개(법률요구, 공중건강활동, 학대, 경시, 가정폭력, 의료감시, 사법, 행정처리, 법률시행, 고인, 장기기증, 연구, 보험 등) 프라이버시 통지 의무기록에 대한 프라이버시 요청권리 의무기록에 대한 개개인의 접근권리 의무기록 개정, 공개 보고, 관리
OECD의 개인정보보호 8원칙	수집제한의 원칙, 정보내용 정확성의 원칙 목적 명확화의 원칙, 이용제한의 원칙 안전보호의 원칙, 공개의 원칙 개인 참가의 원칙, 책임의 원칙

서 형태의 의무기록 보호에 모두 적용된다.

2.1.4 OECD(Organization for Economic Co-operation and Development)의 개인정보보호 지침

1980년 9월 경제협력기구(OECD)는 국가간의 합법적이고 자유로운 정보유통 및 정보처리 산업의 보호를 도모할 목적으로 '프라이버시의 보호와 개인정보보호의 국제적 유통에 대한 지침'을 이사회 권고의 형식으로 채택하였다(OECD 2001). 지침의 내용에 포함된 '국내 적용에 있어서의 개인정보보호의 8원칙'은 회원국에 권고하는 최소한의 기준으로, 각국의 개인정보보호 관련 법·제도 및 지침 등의 모델이 되었으며, 각국의 공공부문이나 민간부문에 광범위하게 받아들여지고 있다.

〈표 1〉은 국내외 개인정보보호 관련 법·제도에서 개인정보보호 항목을 정리한 것이다.

2.2 전자의무기록

2.2.1 전자의무기록(Electronic Medical Record)의 정의

미국 의무기록협회(Medical Record Institute 2005)에서는 '환자의 진료행위를 중심으로 발생한 업무상의 자료나 진료 및 수술검사 기록을 전산에 기반해 입력·정리·보관하는 시스템'이라고 통칭하였으며, 미국의학협회(American Medical Association)에서는 '정확한 자료를 제공하고 의료인에게 필요한 정보를 주어 임상결정을 도와주기 위한 병원정보 시스템이나 처방전달 시스템의 내부에 포함되어 있는 전자적 형태의 환자기록'이라고 정의하였다.

또한 ISO/TC 215 WG 1(International Organization for Standardization/Technical Committee 215 Working Group 1)은 '환자의 기록을 작성, 사용, 저장 및 재생할 수 있는 기능을 보유하는 구성요소의 집합체'로 규정하였다.

〈표 2〉 HL7 EHR SIG에서 정의한 EHR 기능

대 분 류	세부업무	주요 기능
C.1 진료 관리	C.1.1.0 진료정보 획득, 관리, 검토	의료제공자에게 환자기록 식별 및 위치 제공, 환자 인적사항 획득, 문제 리스트 관리, 처치 리스트 관리, 알레르기 리스트 관리, 기타 요약 리스트 관리, 환자력 관리, 차트 요약 검토, 기타 중요 데이터 획득, 임상 문서와 기록의 획득 및 생성, 외부 임상 문서 생성, 환자 제공 데이터 획득, 병력 데이터 획득
	C.1.2.0 진료계획, clinical paths, 프로토콜	임상 가이드라인 제시

(다음 페이지에 계속)

C.1 진료 관리	C.1.3.0 처치 지시와 관리	처치 지시, 처치 규정 지원, 처치 관리 문서화
	C.1.4.0 처치, 이송, 결과 관리	진단 테스트 지시, 다른 지시와의 의사교환, 지시 집합 사용, 이송 지시와 추적, 결과 발송과 관리, 혈액 산물 지시
	C.1.5.0 동의와 인증	동의와 인증 관리, 환자의 이전지시에 대한 획득 · 관리 · 접근
C.2 임상 의사 결정 지원	C.2.1.0 의료정보 획득 및 검토	표준 판단 지원, 환자 콘텍스트 기반 판단 지원, 예외와 잠재적 문제 확인 지원, 환자와 가족의 선호도
	C.2.2.0 진료계획, clinical paths, 프로토콜	표준 질병 기반 프로토콜 지원, 콘텍스트 민감 질병기반 프로토콜 제공, 진행 중인 관리 지원, 표준 프로토콜의 편차 확인 표준 만성질환 관리 기반 프로토콜 지원, 콘텍스트 민감 만성질환 관리 지원, 진행 중인 만성질환 관리 지원, 만성질환 관리 프로토콜의 편차확인 지원
	C.2.3.0 처치 및 관리	처치지시 지원, 처치 관리 지원
	C.2.4.0 처방, 이송, 결과 및 진료 관리	비처치 지시 지원, 결과 해석 지원, 이송 지원, 진료전달 지원
	C.2.5.0 의료 관리 : 예방적 의료와 건강관리	예방 서비스와 건강관리 지원, 예방 서비스와 건강관리를 위한 상호작용 reminder 제공
	C.2.6.0 지원 기능	환경/인구 모니터링 지원, 통지와 응답 지원, 모니터링과 에스컬레이션 지원, 임상 가이드라인 지원, 환자의 지식접근 지원
C.3 운영 관리와 의사교환	C.3.1.0 임상 work flow tasking	업무를 관련 의무기록 입력과 연결, 임상 업무 전달, 임상 업무 추적
	C.3.2.0 임상 의사교환	의료제공자간 의사교환, 약국 의사교환, 제공자/환자/가족 의사교환, 환자, 가족, 간병인 교육, 의료장비와의 통신
S.1 임상 지원	S.1.1.0 질병 등록소	
	S.1.2.0 공여자 관리 지원	

(다음 페이지에 계속)

S.1 임상 지원	S.1.3.0 제공자 위치	제공자 인적사항 관리, 시설 위치, 전화 위치, 일반 위치
	S.1.4.0 환자 위치	시설 내에서 환자 위치, 서비스 제공 및 관리 관련된 환자 주거, 환자 침상정리 최적화
	S.1.5.0 인적사항과 비식별 정보	환자 인적사항, 비식별 데이터 요청 관리
	S.1.6.0 스케줄링	
S.2 관리, 분석, 연구, 보고	S.2.1.0 관리, 모니터링, 분석	결과 관리, 진료 지표, 성능과 책임성 기준
	S.2.2.0 보고서 생성	
	C.2.3.0 처치 및 관리	처치지시 지원, 처치 관리 지원
S.3 관리와 재정	S.3.1.0 진료 관리 encounter/에피소드	특정 뷰, encounter 특정 기능성, 임상 데이터와 관리, 재정 데이터 통합, 장비 모니터링과 원격의료 데이터 같은 원거리 의료 서비스 통합
	S.3.2.0 추가이용을 위한 정보 접근	규칙-구동 임상 코딩 지원, 규칙-구동 재정, 관리 코딩 지원, 비용 관리 정보 통합, 처방집 의사교환
	S.3.3.0 관리 트랜잭션 처리	환자 등록, 자격 확인과 보상범위 결정, 서비스 인증, 서비스 요청과 지불 요구 지원, 배상을 위한 지불요구와 encounter 보고, 진료 종결시 의료 서비스 보고, 임상, 관리 응답과 승인의 수령
	S.3.4.0 개업의/환자 관계	개업의 지정, 환자 리스트 관리
	S.3.5.0 환자와 다른 사람과의 관계	가계 관련, 보험 관련, 주거상태 관련, 다른 수단 관련
	S.3.6.0 급성과 중함	환자 질병/위험 조정의 급성/중함, 제공자 스탭 레벨 조정
	S.3.7.0 EHR 지원내용 자동 갱신	임상 의사결정 지원 시스템 가이드라인 갱신, 환자 교육자료 갱신, 환자 reminder 정보 갱신, 의사의 지속적인 교육 정보 갱신, 공중 건강관련 갱신

(다음 페이지에 계속)

I.1 Information Infrastructure	I.1.1.0 EHR 정보 보안	대상 인증, 대상 권한부여, 자원 데이터 교환, 환자 프라이버시
	I.1.2.0 EHR 정보관리 (기록 관리)	정보 무결성, 문서 유지, 가제본 문서, 문서 증거, 기밀성, 감사추적, 데이터 보관 및 저장
	I.1.3.0 Chain of Custody	
	I.1.4.0 유일 식별자, 등록, 디렉토리	등록간 커뮤니케이션, 임상기능을 위한 대상 식별 색인, 임상기능을 위한 대상 식별 관리, 대상 접근 검색, EHR 중요 디렉토리, 임상 등록소, 자원과 위치 검색
	I.1.5.0 용어 기능	표준 용어, 일관성 있는 용어, local 용어 매핑, 코드 집합 관리, 코드 집합 Versioning
	I.1.6.0 상호운용성	상호작용-모델 기반 교환, Chain of Trust, 표준기반 상호운용성, 동기화, EHR 데이터 추출, 임상 문서
	I.1.7.0 비즈니스 규칙 관리 기능	비즈니스 규칙 관리, 비즈니스 규칙 수행/적용, 비즈니스 규칙의 무효화, 비즈니스 규칙 사용 감사
	I.1.8.0 작업흐름	작업 분산, 시스템 트리거 업무 routing, 작업흐름 업무 할당

2.2.2 전자의무기록의 기능

1) 기능 정의의 필요성

대부분의 전자의무기록 또는 전자건강기록 시스템은 업체 종속적이며 다양하기 때문에, 이의 기능에 대한 공통 요구사항을 도출하는 것이 의료기관의 입장에서는 업체에서 제공하는 시스템들을 비교하는데 유용하고, 업체의 입장에서는 의료기관의 기대치를 달성할 수 있다.

2) 기능 정의

전자의무기록의 최종목표 시스템인 전자건강기록(EHR) 시스템에 대한 기능을 정의하는 과정에서 2001년 결성된 HL7 EHR SIG(HL7 Electronic Health Records Special Interest Group)에서는 〈표 2〉와 같이 정의하였다.

또한 국내에서는 2004년 대한의료정보학회 춘계학술대회에서 전자건강기록 시스템에 대한 기능을 〈표 3〉과 같이 정의하였다(김윤연 2004).

2.2.3 국내외 전자의무기록 도입현황

1) 미 국

2003년 미국에서 1차 진료의 5%만이 전자의무기록 시스템을 사용하고 있었다. 그런데 2003년 3월 부시 대통령은 상호운용성을 지닌

〈표 3〉 대한의료정보학회에서 정의한 EHR 기능

대 분 류	주요 기능
1. 직접 환자진료 정보	환자진료시에 필요한 정보지원, 치료계획 · 표준진료일정 · 표준진료지침, 지식기반 의사결정지원, 처방관리, 결과관리, 투약처방 및 투약관리, 간호기록 및 중재관리, 검체 채취 및 관리, 알레르기 및 투약부작용 관리,유의사항 및 주의사항 관리, 건강증진 및 예방정보관리, 동의서 및 허가서 관리, 환자 임상문제 및 상병관리, 식이 급식 관리, 진료업무관리
2. 진료업무 및 운영관리	진료업무 관리, 일정관리, 작업대장 관리
3. 관련자간 통신 및 의사소통	의사간 통신, 팀 조정, 주치의와 환자/가족 간 통신, 환자교육, 의무기록정보 교환, 의료장비 연결 접속, 외부 약국 연결 접속, 외부 위탁검사실 연결접속, 의료보험회사 연결 접속
4. 기록, 문서 및 조회	의무기록 조회, 타임 스탬프 관리, 병력관리, 영상 관리, 생체신호 관리, 스캔 문서 관리, 사진 관리, 소리 관리, 임상문서 관리, 원거리 접속, 정신과 특수기록 보호, 의사/개인 사용일지 관리, 반복 조회
5. 임상지원	역학적 감시 관리, 상병등록 관리, 혈액은행 공혈자 관리, 환자위치 탐지, 전문의 탐지, 환자 이동 관리, 환자임상 관리, 신상정보 암호화 관리
6. 분석, 측정 및 결과	진료의 질 지표 관리, 업적 및 책임 측도 관리, 분석 및 측정 관리, 보고서 및 보고 관리, 임상시험 연구 관리
7. 행정, 재정	환자외래 진료행위 관리, 환자보험자료 및 진료의뢰 관리, 환자와 의사의 관계, 환자 가족 연계 관리, 상병 · 진료결과 코드 관리, 환자 진료비 관리, 비용관리, 지역 유관기관 관리, 보험진료비 청구 및 진료비 청구관리
8. 정보보호	개인정보 비밀 보호, 보안
9. 기록관리	환자기록 히스토리 관리, 환자 의무기록 관리, 보내온 의무기록 관리, 외부로 보내는 의무기록 관리, 의무기록 생성 및 생명주기 관리, 의무기록의 동시성 관리, 기록 관련 인물 연계 관리
10. 등록관리	환자 등록 및 마스터 인덱스 관리, 의사 등록 관리, 역할 등록 관리, 엔터티 등록 관리, 소재지 등록 관리
11. 의무기록 기술적인 기반구조	전자의무기록 이용 가능성 관리, 전자의무기록 버전 관리
12. 용어 코드 관리	LOINC · SNOMED · ICD · 보험청구 코드 등 관리된 코드
13. 데이터베이스 관리	데이터베이스 백업 관리, 데이터베이스 복구 관리, 데이터베이스 완전성 관리

(다음 페이지에 계속)

14. 데이터베이스 트랜잭션 관리	대형 트랜잭션 관리, 신속한 트랜잭션 처리 관리, 다단계 데이터베이스 처리, 다 노드 동시 기록, 트랜잭션 저널링
15. 온라인 트랜잭션 처리	온라인 트랜잭션 처리 관리
16. 장애 내구성 및 중복성	장애 내구 아키텍처, 중복자료 저장
17. 사용자 응답 시간	시스템 반응 관리
18. 전자의무기록 시스템 이식성	필요에 따른 이식성 관리
19. 시간의 동시성 관리	다양한 전자의무기록 시스템 간의 동시성 관리
20. 사용자 환경	전자의무기록 생성 환경, 전자의무기록 개발 및 시험환경, 전자의무기록 사용자 교육 환경

전자건강기록(EHR)의 지원을 발표하였으며, 2004년 4월에는 국가 전자건강기록 인프라 구축을 위한 10년 계획을 수립하였다. 이를 통해 "always current, always available EHR"을 향한 4개 목표와 12개의 전략을 설정하여 단계적으로 추진 중이다(김동수 2004).

2) 영 국

1999년 설립된 e Health 협회를 중심으로 통합 의무기록 서비스(Integrated Care Records Service)를 2008년까지 3단계로 나누어 구축 진행 중이며, 2003년 98%의 개업의가 컴퓨터에서 전자의무기록에 접속할 수 있고, 이 중 30%가 종이기반 의무기록을 없애고 있다(김동수 2004).

3) 호 주

2000년 5월 70%의 개업의가 진료실에 컴퓨터를 도입하였다. 이는 1997년 10월의 15% 도입에 비하여 매우 비약적인 성과를 나타내고 있으며, 정부에서는 컴퓨터 구입에 따른 재정지원, 필요 시스템 지원, 전자청구시의 인센티브 제공 등을 지원하고 있다(김동수 2004).

4) 일 본

후생성은 2001년 12월 보건의료 분야 정보화를 위한 "Grand Design"을 발표하고, 전자의무기록 등의 연차별 추진목표설정 및 지원추진 중이다. 2004년까지 전국 2차 의료권의 최소 1개 기관에 전자의무기록을 보급하고, 2006년까지 400병상 이상 병원의 60%에 보급할 예정이다(김동수 2004).

5) 국내 도입현황

정부에서 2002년 3월, 의료법 제21조의 2(전자의무기록)에서 "진료기록부 등을 전자서명법에 의한 전자서명이 기재된 전자문서로 작성·보관할 수 있다"고 규정한 이후, 현재 전자

의무기록을 도입한 의료기관의 경우, 신규로 발생하는 의무기록은 전산으로 입력, 저장, 사용하고 있으며, 기존 의무기록은 이미지 파일로 저장, 사용하고 있다.

의료기관의 경우, 전자의무기록에 대한 개념이 다소 차이를 보이지만, 전사적 차원에서 전자의무기록을 도입한 병원은 분당 서울대병원을 비롯해 대구 동산의료원, 분당 제생병원, 인하대병원 등을 꼽을 수 있으며, 서울 아산병원과 삼성서울병원도 부분적으로 도입하고 있다. 이외에도 연세의료원 등의 종합병원과 제주한국병원 등의 중소병원에서도 도입하고 있는 추세이다(한림의료원 2004).

2.3 보안(Security)

2.3.1 PKI(Public Key Infrastructure)

자료에 대한 암호화를 하는 주체와 그 자료를 복호화하는 대상이 동일한 키를 사용하는 대칭 키 암호기술은 그 알고리듬의 구조상 암복호화의 시간이 짧게 소요되고, 사용이 용이하다는 이유로 많이 사용되고 있다. 그러나 키 관리 등의 어려움으로 이를 보강하기 위한 새로운 개념인 공개 키 암호기술이 생성되었다.

공개 키 암호 기술에서는 비밀 키와 공개 키를 이용한다. 먼저 사용자는 공개 키와 이에 대응하는 비밀 키를 생성한다. 비밀 키는 그 키를 소유하고 있는 주체만이 알고 있고 공개 키는 공개된다. 그런데 불특정 다수에게 공개된 공개 키가 위·변조되지 않도록 무결성을 보장하기 위해 등장한 내용이 공개 키 기반구조(PKI: Public Key Infrastructure)이다. 공개 키 기반구조에서는 공개 키를 공개하면서 공개 키와 키의 소유자와의 관계를 생성하고 이에 대한 인증 및 무결성을 보장하기 위해서 전자서명이라는 방법을 사용한다. 즉, 전자서명된 인증서와 키의 주체가 소유하고 있는 개인 키를 사용하는 것이 PKI이다.

PKI에서 제공되는 기본 보안 서비스는 다음과 같다(이만영 외 1999).

1) 기밀성: 대칭 키 및 비 대칭 키를 사용하고 자료에 대한 암호화를 통해 기밀성을 제공한다.

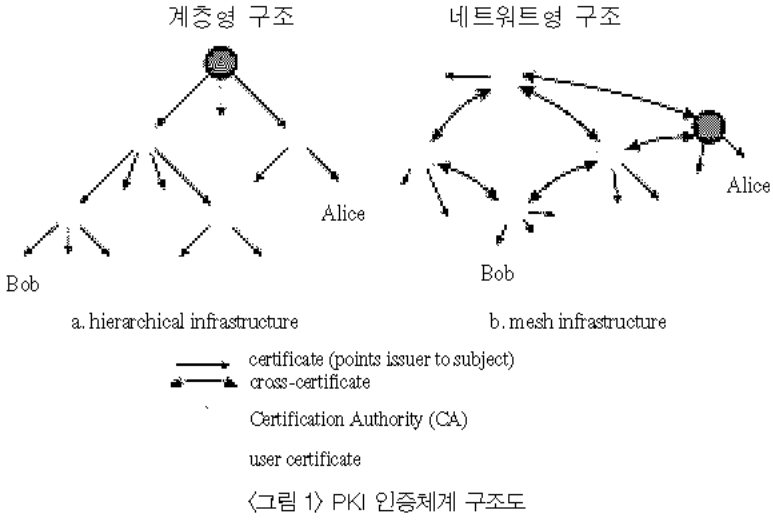
2) 접근제어: 키를 소유하고 있는 대상만이 정보에 접근할 수 있도록 한다. 즉, 공개된 키로 암호화 한 것은 공개 키와 한 쌍을 이루고 있는 개인 키를 소유한 사람만이 정보를 복호화 하여 내용을 확인할 수 있도록 한다.

3) 무결성: 해시(hash) 함수 등을 사용하여 정보가 중간에 누군가에 의해 수정·변경되지 않도록 한다.

4) 인증: 정보를 구성한 주체에 대한 확인을 할 수 있는 방법을 제공한다. 정보를 구성한 주체가 전자서명을 통해 생성을 하고 이를 인증서에 있는 공개 키로 검증하는 과정에서 이루어진다.

5) 부인방지: 향후 분쟁이 생성되었을 경우, 정보를 구성한 주체가 누구인가를 확인하는 과정에서 정보구성주체자를 확인할 수 있다.

PKI 구조는 <그림 1>과 같이 인증기관 간에



〈그림 1〉 PKI 인증체계 구조도

계층을 형성하여 상위 인증기관 간의 상호인증은 허용하고, 하부의 인증기관 간의 상호인증은 허용하지 않는 계층구조(Hierarchical Infrastructure)가 있으며, 인증기관 간에 동등한 평면적 구조로 모든 인증기관 간 상호인증을 허용하는 네트워크 구조(Network Infrastructure)가 있다(한국정보보호진흥원 2004). 국내는 한국정보보호진흥원이 최상위 인증기관(Root CA)이며, 산하에 공인인증기관인 한국정보인증, 한국증권전산, 금융결제원, 한국전산원, 한국전자인증 등이 존재하는 계층구조로 인증체계가 이루어져 있다.

2.3.2 전자서명의 원리

전자서명의 대략적인 흐름은 〈그림 2〉와 같다(한국정보보호진흥원 2004).

전자서명을 할 자료에 대하여 일방향함수인 해시 함수를 통해 자료에 대한 값을 구한다. 해당 해시 값을 사용자의 개인 키로 암호화를 한다. 이 정보를 송신자의 공개 키와 함께 수신자에게 보낸다.

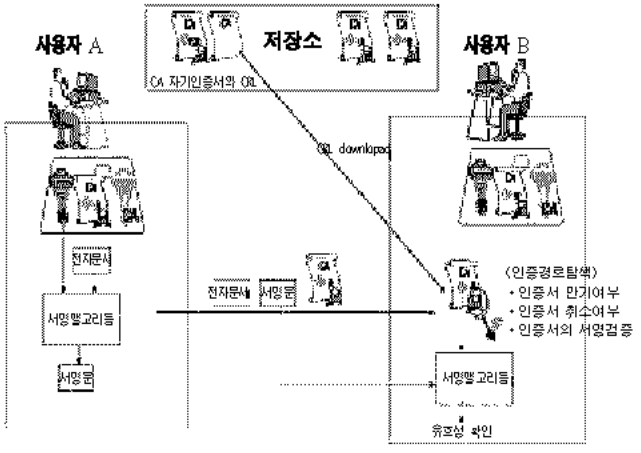
수신자는 자료를 수신하였을 경우 원래의 자료를 해시 알고리듬을 통하여 해시 값을 구한다. 수신된 송신자의 공개 키가 있으므로 그 공개 키를 사용하여 암호화된 해시 값을 복호화하여 미리 구한 해시 값과 비교하여 자료가 수정되지 않았음을 검증한다.

2.3.3 인증서 개념

인증서는 공개 키 소유자의 신분과 공개 키와의 관계를 증명해 주는 전자문서이다.

〈그림 3〉은 인증서의 형식을 도식화한 내용이다(Housley et al. 1999).

공개 키와 공개 키 소유자에 대한 정보를 함께 묶어놓은 전자문서가 인증서인데, 이러한 정보는 쉽게 수정될 수 있어, 자료에 대한 무결성



〈그림 2〉 전자서명 개념도

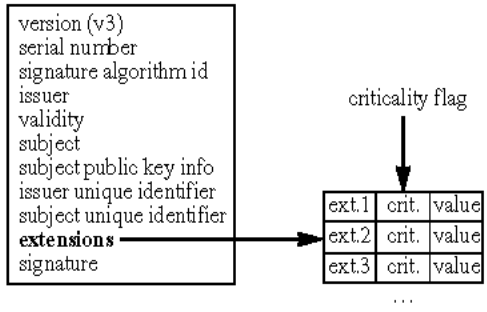
이 무엇보다 중요하다. 때문에 전자서명의 원리가 인증서에 적용된다. 이때 전자서명에 대한 정당성을 부여하기 위해 신뢰할 수 있는 인증기관이 자신의 비밀 키로 전자서명을 하여 생성한다. 즉, 인증서의 유효성은 위에서 설명한 전자서명의 기본원리를 이용하고 신뢰할 수 있는 인증기관이 서명한 것이다. 〈그림 3〉에서 보면 공개 키의 소유자인 subject와 subject public key info 내의 공개 키와의 관계를 신뢰할 수 있는 issuer가 자신의 비밀 키를 사용하여 서명한 signature를 포함하고 있다.

2.3.4 개인정보보호와 전자서명

현재 사회전반에 걸쳐 확산, 가속화되고 있는 정보화 과정은 사회통제의 수단과 통제기관의 효율성 및 통제적 잠재력을 전반적으로 크게 향상시키고 있으며, 이에 따라 개인 프라이버시 침해의 문제는 정보사회로 이동하면서 사회적인 문제가 되고 있다. 정보사회의 위험요소로 프라이버시 침해가 특히 부각되는 이유는 크게 두 가지 측면에서 논의될 수 있다. 하나는 정보의 디지털화로 인해 개인에 대한 사회적 감시기술 자체가 획기적으로 발전하고 있다는 기술적 측면과, 또 하나는 정보사회 및 신용사회의 도래와 함께 개인 신상정보에 대한 사회적 수요가 급증하는데 따르는 사회적 측면의 변화이다.

때문에 개인정보보호는 사회에 의해 생성된 개인정보의 생성, 유통, 수정 및 소멸의 과정이 사회적인 규정과 제도의 틀에 의해 이루어져야 하며, 이를 위한 기술적인 장치가 마련되어야 한다(이동훈 2003).

전자서명은 2.3.1절의 PKI 기술이 제공하는 서비스를 만족하고 있다. 문서의 생성, 수정 및 소멸시 주체를 인증할 수 있는 기능 및 행위에 대한 부인방지기능을 제공한다. 또한 생성된 문서에 대한 무결성 및 기밀성을 제공하고 있다.



〈그림 3〉 인증서 형식

때문에 ISO17799 및 BS7799 등 정보보안관리 규범에서도 응용 시스템 보안을 위해서 PKI 기반하의 관련기술의 적용을 규정하고 있다.

2.3.5 인증기관

인증기관은 개인의 신분증을 발행하는 행정기관적인 성격으로 전자서명을 하기 위한 개인키와 인증서에 대한 신뢰성을 제공하는 기관이다. 즉, 공개 키와 공개 키의 소유자에 대한 정보를 인증기관의 개인 키로 전자서명을 한 결과인 인증서를 발급한다. 전자서명의 원리에 의해 신뢰할 수 있는 기관만이 신뢰할 수 있는 인증서를 발급할 수 있다. 때문에 인증기관은 전자서명을 하기 위한 개인 키에 대한 보호대책 및 개인에 대한 본인확인 대책을 철저히 마련하여야 한다.

인증기관의 필요성은 다음과 같다.

① 불특정 다수의 전자서명 키에 대한 인증을 수행

② 전자서명 키에 대한 대외 공신력을 제공

③ 전자문서 이용관련 분쟁의 최소화

〈표 4〉와 같이 개인의 신분증과 유사한 인증서에 대해 온라인 상으로 신뢰성을 보장받기 위해서는 신뢰할 수 있는 인증기관의 역할이 무엇보다 중요하다.

3. 개인의료정보 보호방안 수립

의료분야의 전자의무기록에 대한 보안표준화를 수립하기 위해서는 의료분야에 맞는 개인정보보호에 대한 정의 및 범위가 먼저 설정되어야 한다.

따라서 본 장에서는 의료분야에서의 개인정보보호에 대한 적용범위를 "개인의료정보"로 규정, 개인의료정보 사용·공개에 관한 범위를 설정하고, 개인의료정보에 대한 개인의 권리를 정의하였다. 이는 HIPAA 개인정보보호규정을 근간으로 하고, 국내 의료기관이 공동 발의한 의료정보윤리헌장을 참조로 하여 관련학회, 시민단체 및 전문가들의 의견수렴과 검증을 통해 개인의료정보 보호방안을 수립하였다.

3.1 개인의료정보의 정의

개인의료정보는 개인의 신체적, 정신적 상태

〈표 4〉 신분증과 인증서 비교

구분	off-line	on-line
신분증발급	- 행정기관, 군부대, 기업체 등의 인사담당 부서	- 인증기관의 인증서(운영/관리기관)
신분증확인	- 통제구역 출입, 검문, 금융기관에 제시 - 각종 증명서 발급시 제시	- 전자서명된 자료와 함께 제시
기명날인	- 결제, 계약서 완성 - 발주서, 물품수령 확인	- 전자서명된 자료를 유효한 인증서의 공개 키로 검증

나 기능적 상태에 관한 예방, 진단, 치료 및 재활과 관련된 의무기록, 연구결과 정보, 의학정보 및 원무정보 모두를 말한다.

3.2 기본 전제

1) 의료정보 주체의 이익 우선

개인의료정보의 보호는 의료정보 주체(의료정보의 대상이 되는 개인)의 이익이 우선 고려되며, 정보의 전문적, 공익적 활동에 우선하여 보호한다.

2) 의료정보 주체와 의료정보 관리자의 노력

개인의료정보의 보호를 위하여 의료정보 주체, 의료정보 관리자(의료정보 생성, 보관, 관리 및 유통에 책임과 권한을 가진 자)가 공동으로 노력한다.

3.3 개인의료정보의 사용 · 공개

1) 합목적적 사용

개인의료정보는 그 정보를 생성한 목적에 맞도록 사용되어야 하며, 정보의 사용과 공개, 정보에 대한 접근 및 정정 · 보정 권한 등을 지정함에 있어 전문성과 공익성을 고려한다.

2) 최소공개의 원칙

개인의료정보는 정보가 필요한 사람에게, 필요한 정보에 한하여 공개하는 것을 원칙으로 한다. 다만, 개인의 정당한 요구가 있거나, 개인의 건강과 이익을 지키기 위한 경우에는 예외로 한다.

3) 개인식별이 가능한 의료정보의 공개 금지

개인식별이 가능한 의료정보는 개인의 성명, 주소, 생년월일, 주민등록번호, 전화번호, 우편번호, 전자우편 주소, 의무기록번호, 사진 등 의료정보 주체를 식별할 수 있는 내용이 포함된 정보를 말한다.

개인식별이 가능한 상태에서 개인의 과거, 현재, 미래의 신체적, 정신적 건강상태, 치료내용과 의료비용 발생 내역이 공개되어서는 아니 된다.

4) 개인식별이 불가능한 의료정보의 허용

개인식별이 불가능한 의료정보는 개인의 식별이 가능한 의료정보 및 개인의 가족, 친척, 직장동료 등 관련자의 개인식별이 가능한 의료정

보가 포함되어 있지 않은 정보를 말한다. 의료정보 관리자가 데이터베이스나 전문적인 기술을 이용해야만 개인식별이 가능한 의료정보는 개인식별이 불가능한 것으로 간주한다.

5) 비밀누설의 금지

① 의료정보 관리자는 개인의 기밀정보를 관리하는 의료정보 관리자로서의 책임과 의무를 다한다.

② 의료정보 관리자는 의료, 조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못한다.

③ 의료정보 관리자는 개인의료정보 보호를 위하여 필요한 기술적, 제도적 조치를 취한다.

6) 의료정보 관리자의 판단으로 사용 · 공개 가능한 개인의료정보의 범위

① 개인의 치료, 의료비 지불, 진료내용 평가에 필요한 경우

② 개인이 거부하지 않았다고 인정할 수 있는 다음의 경우

입원시 의무기록의 병실 내 열람

응급시 의무기록의 열람

의식이 없는 경우 의무기록의 열람 등

③ 수사나 재판 등 법률적인 절차에 의하여 요청된 경우

④ 의료정책 수립과 수행 등 사회 공공의 이익에 합치된다고 판단하는 경우

⑤ 산업재해 등에 해당하여 개인의 이익을 보호하는 데 필요하다고 인정하는 경우

⑥ 사망한 개인에 대한 정보를 장기기증, 장의사, 수사 기관 등에서 요구하는 경우

⑦ 다음과 같은 정신과 치료기록의 경우

정신과 치료를 위해 치료기록 최초작성자가 사용하는 경우

학생 · 수련의의 임상교육이나 기술향상을 위해 의료정보 관리자가 사용하는 경우

개인의 소송에 대해 의료정보 관리자의 변호를 위해 사용하는 경우

7) 연구목적으로 사용 · 공개 가능한 개인의료정보의 범위

① 연구목적과 방법 및 내용이 개인의 이익에 배치되지 않는다고 의료정보 관리자가 인정한 경우

② 연구수행을 준비하는 단계에서 일시적으로 필요한 정보라고 연구자가 요청하는 경우, 단, 그 필요성이 충족된 후에는 해당 정보를 폐기하여야 한다.

③ 사망한 개인의 의무기록을 연구용으로 쓰고자 하는 경우

8) 개인의료정보 사용 · 공개시 개인의 서면동의를 받아야 하는 경우

① 개인의료정보가 포함된 정보를 사용 · 공개할 때는 개인의 서면동의를 받아야 한다. 다만, 앞의 6)에서 기술한 '의료정보 관리자의 판단으로 사용 · 공개 가능한 개인의료정보의 범위'와 7)에서 기술한 '연구목적으로 사용 · 공개 가능한 개인의료정보의 범위'의 경우에는 사후에 서면동의를 받거나 생략할 수 있다.

② 개인의 서면동의에는 다음의 내용을 명확하게 표시한다.

"이 동의는 개인의료정보가 어떻게 사용 · 공개되고, 개인이 어떻게 접근할 수 있는가를 설명하고 있습니다. 주의 깊게 검토하십시오."

3.4 개인의료정보에 대한 개인의 권리

3.4.1 개인의료정보의 사용 · 공개에 대한 제한요청 권리

개인은 개인의료정보의 사용 · 공개에 대한 제한요청 권리를 가진다. 다만, 개인이 서면으로 그 제한요청이 완료되었음을 승인하거나, 또는 개인의 구두승인을 문서화한 경우에 그 제한요청을 해제한다.

3.4.2 개인의료정보에 대한 접근권리

1) 접근 권리

개인의료정보에 대한 접근 권리를 가질 수 있는 자격은 다음과 같다. 다만, 정신과 치료기록은 개인의 서면 동의를 받아야 한다.

① 의학적 증상의 치료 · 검사를 위하여 의료정보 관리자로부터 의료를 제공받은 본인

② 본인이 요청할 수 없는 경우에는 배우자 · 직계존비속 또는 배우자의 직계존속

③ 그 배우자 · 직계존비속 및 배우자의 직계존속이 없거나 질병, 기타 요청을 할 수 없는 부득이한 사유가 있는 경우에는 본인이 서면으로 대리인으로 임명한 자

④ 개인이 미성년인 경우에는 양친 또는 후견인

2) 접근요청 및 조치

① 개인은 자신의 의료정보에 대한 접근을 서면으로 요청한다. 접근요청을 받은 의료정보 관리자는 요청수령 후 10일 이내에 다음의 조치를 취한다.

의료정보 관리자는 접근요청을 허가한 개인에게 요청승인을 고지하고, 요청된 접근을 제공한다.

당해 의료정보 관리자가 당해 정보를 보관하고 있지 않은 경우에는 이를 개인에게 알리고, 판명되고 있는 경우에는 당해 정보를 보관하고 있는 의료정보 관리자의 명칭 · 주소를 알려준다.

의료정보 관리자가 접근요청을 거부하는 경우, 개인에게 그 사유 등을 명시하여 서면으로 고지한다.

② 의료정보 관리자는 개인이 접근을 요청한 기한 내에 조치를 취할 수 없는 경우, 개인에게 지연사유 및 의료정보 관리자가 요청에 대한 조치를 완료할 수 있는 기간에 대하여 서면으로 고지하고, 1회에 한하여 그 기간을 10일 이내로 연장할 수 있다.

③ 의료정보 관리자는 개인이 접근을 요청하는 시간, 장소 및 방법으로 개인의료정보를 제공한다.

④ 의료정보 관리자는 개인이 요청한 형식으로 개인의료정보를 제공한다. 다만, 요청한 형식이 쉽지 않은 경우, 의료정보 관리자와 개인이 동의한 다른 형식으로 제공할 수 있다.

⑤ 의료정보 관리자는 개인의 접근요청에 대하여, 당해 의료정보 관리자가 유지하고 있는 최신의 완전한 정보를 개인이 이해할 수 있

을 것이라고 합리적으로 기대할 수 있는 용어 · 언어로 제공한다.

⑥ 개인이 개인의료정보 사본을 요청하는 경우, 다음 비용을 포함한 적정의 비용을 부과할 수 있다.

개인이 요청한 개인의료정보의 복사비

개인이 우편으로 요청한 경우의 우편료

3) 접근거부

개인은 다음의 경우에 자신의 의료정보에 대한 접근 권리가 허용되지 않는다.

① 요청된 접근이 개인 자신이나 다른 사람의 생명이나 신체안전을 저해한다고 전문가적인 견해에서 의료정보 관리자가 판단한 경우

② 교정기관의 지도하에서 활동하는 의료정보 관리자가 개인의료정보에 대한 접근권리 허용이 개인 자신이나 다른 수감자의 의료, 안전, 보안, 수감, 재활, 또는 교정기관 종사자 등의 안전을 위협한다고 판단한 경우

③ 개인이 치료를 포함한 연구에 참여하기로 동의하고 접근거부에 찬성한 경우. 다만, 치료를 포함한 연구과정에서 의료정보 관리자가 생성 또는 획득한 의료정보에 대한 개인의 접근은 연구가 진행되는 동안 일시적으로 중단되나, 연구완료 후에는 개인의 접근권리가 회복되어야 한다.

3.4.3 개인의료정보에 대한 정정 · 보정 요청권리

1) 정정 · 보정 요청권리

개인은 개인의료정보가 의료정보 관리자에게 유지되는 동안 부정확 · 불완전하다고 판단되는 경우에 그 정정 · 보정 요청의 권리를 가진다.

2) 정정 · 보정 요청 및 조치

① 개인은 자신의 의료정보에 대한 정정 · 보정을 서면으로 요청하며, 정정 · 보정 요청을 받은 의료정보 관리자는 요청 수령 후 30일 이내에 다음의 조치를 취한다.

의료정보 관리자는 정정 · 보정 요청을 허가한 개인에게 요청승인을 고지하고, 정정 · 보정되는 정보를 의무기록 중에 포함시킴과 동시에 정정 · 보정이 된 곳에 날인을 하여 그 위치를 표시한다. 부정확 · 불완전한 정보에는 날인할 뿐, 그것을 삭제해서는 아니 된다.

의료정보가 존재하지 않거나 또는 발견할 수 없는 경우에는 이를 개인에게 알려준다.

당해 의료정보 관리자가 당해 정보를 보관하고 있지 않으나, 당해 정보를 보관하고 있는 의료정보 관리자를 인지하고 있는 경우에는 해당 의료정보 관리자의 명칭 · 주소를 개인에게 알려준다.

② 의료정보 관리자가 정정 · 보정 요청을 거부하는 경우, 개인에게 그 사유 등을 명시하여 서면으로 고지하고, 요청된 정정 · 보정 및 그 요청거부사유를 의무기록 중에 포함시킴과 동시에, 부정확 · 불완전한 정보를 사유로 신청된 경우, 개인이 주장하는 곳에 날인하여 개인의 이의가 있음을 표시한다.

③ 의료정보 관리자는 당해 의료정보가 사용 중

에 있는 경우 또는 예외적인 사정 때문에 정정·보정 요청의 처리가 늦어지는 경우, 개인에게 지연사유 및 의료정보 관리자가 요청에 대한 조치를 완료할 수 있는 기간에 대하여 서면으로 고지하고, 1회에 한하여 그 기간을 30일 이내로 연장할 수 있다.

3) 정정·보정 요청거부

의료정보 관리자는 개인이 의료정보의 주체라는 믿을 만한 근거를 제공하지 않거나, 의료정보가 정확하고 완전한 경우, 정정·보정에 대한 개인의 요청을 거부할 수 있다.

4. 전자의무기록 보안표준화 수립

2.3.4절의 관련연구를 통해 정보를 보호하기 위해서 전자서명의 필요성을 언급하였다. 디지털 형태로 생성되는 전자의무기록은 보호되어야 할 개인정보를 포함하고 있고, 개인정보보호를 위해서 전자의무기록에 대한 전자서명의 적용을 검토할 필요가 있다. 또한, 관련법률을 검토하여 전자의무기록에 대한 전자서명의 법적 효력을 확보하여야 한다.

따라서 본 장은 3장에서 수립된 개인의료정보 보호방안을 근거로 전자의무기록에 대한 보안표준화 수립을 위한 전자의무기록 관련 법률을 재해석하여 검토사항을 도출한다. 그리고, 전자의무기록에 전자서명을 적용하기 위한 세부사항을 예시하며, 전자의무기록 시스템에 전자서명 적용을 위한 지침을 마련한다.

4.1 개인의료정보 보호를 위해 전자의무기록 관련 법률 검토사항

〈표 5〉는 전자의무기록 관련 법률에서 보안 적용을 위해 추가적으로 검토되어야 할 사항을 제시하였다. 무엇보다 전자의무기록이 전자문서형태로 작성이 되어야 할 경우에는 신뢰할 수 있는 인증기관이 발급한 인증서를 이용해서 전자서명이 되어야 한다. 이는 전자문서를 생성시점부터 소멸까지 그 정보의 변조 및 훼손을 방지함은 물론, 문서를 작성한 주체에 대한 신원확인 및 부인방지를 통해 전자의무기록의 오·남용을 방지할 수 있기 때문이다. 또한 전자의무기록이 보존되는 동안 전자의무기록을 검증할 수 있는 구조가 마련되어야 하며, 전자의무기록을 백업하였을 경우에 대한 대책을 마련하여야 한다.

4.2 전자서명 적용을 위한 세부사항

의료기관에 도입된 전자의무기록 시스템에 전자서명을 적용하기 위해서는 다음과 같은 항목이 변경되어야 할 것이다.

① 전자의무기록에 대한 전자서명 적용절차 도입

② 인증서 기반으로 사용자 로그인 절차변경

③ 저장된 전자의무기록 데이터에 대한 검증절차 도입

④ 전자의무기록에 대한 접근권한 관리 및 보안 관련 재검토

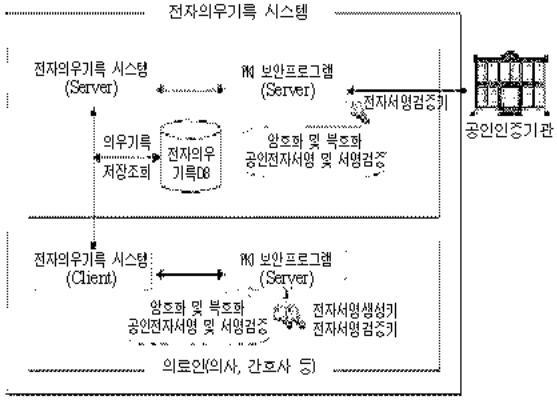
〈표 5〉 전자의무기록 관련 법률 검토사항

현행 법률	검토 사항
• 의료법 제21조 (진료기록부 등) ① 의료인은 각각 진료기록부 · 조산기록부 · 간호기록부 그 밖의 진료에 관한 기록을 비치하여 그 의료행위에 관한 사항과 소견을 상세히 기록하고 서명하여야 한다	- 전자문서일 경우, 전자서명을 적용하여야 함.
• 의료법 제21조 (진료기록부 등) ② 의료인 또는 의료기관의 개설자는 진료기록부 등을 보건복지부령이 정하는 바에 의하여 보존하여야 한다. • 시행규칙 제18조 (진료에 관한 기록의 보존) ① 진료기록부, 수술기록의 법정 보존기간 : 10년 ② 검사소견기록의 법정 보존기간 : 5년 ③ 처방전의 법정 보존기간 : 2년	- 법정 보존기간 중 전자의무기록의 활용이나 검증이 가능하여야 함.
• 의료법 제21조의 2 (전자의무기록) ① 의료인 또는 의료기관의 개설자는 진료기록부 등을 전자서명법에 의한 전자서명이 기재된 전자문서로 작성 · 보관할 수 있다. ② 의료인 또는 의료기관의 개설자는 보건복지부령이 정하는 바에 따라 전자의무기록을 안전하게 관리 · 보존하는데 필요한 시설 및 장비를 갖추어야 한다. • 시행규칙 제18의 2 (전자의무기록 관리 · 보존에 필요한 장비) 의료인 또는 의료기관 개설자는 전자의무기록의 생성과 전자서명을 검증할 수 있는 장비, 전자서명이 있은 후 전자의무기록의 변경여부를 확인할 수 있는 장비, 네트워크에 연결되지 아니하는 백업 저장 시스템을 갖추어야 한다.	- 전자의무기록의 안전한 관리 · 보존에 필요한 시설 및 장비는 소산보관, HDD 백업, CD 백업 등의 구체화 필요
• 의료법 제21조의 2 (전자의무기록) ③ 전자의무기록에 저장된 개인정보를 탐지, 누출, 변조 또는 훼손하여서는 아니 된다.	- 전자의무기록 데이터의 암호화 보존 여부에 대한 검토 필요

⑤ 전자의무기록 데이터에 전자서명 값 추가에 따른 데이터베이스 설계변경

⑥ 전자서명 툴 키트 도입 및 등록기관 기능수행 시 인증서 등록관리 소프트웨어 도입

본 절에서는 위와 같이 전자의무기록 시스템에 전자서명을 적용하기 위한 항목을 고려하여 효과적으로 전자서명을 적용하기 위한 방법을 예시하였다.



〈그림 4〉 전체 시스템 개념도

4.2.1 시스템 개념도

전자의무기록에 대해 전자서명을 적용하기 위하여 가장 먼저 선행되어야 할 것은 신뢰할 수 있는 인증기관을 통해 인증서가 발급되어야 하는 점이다. 개인에 대한 인증 및 전자서명을 위한 공개 키 및 관련정보에 대한 신뢰는 인증기관을 통해 발생하기 때문에 〈그림 4〉에서는 신뢰할 수 있는 인증기관으로 공인인증기관을 예시하였다.

4.2.2 세부사항

1) 인증서 유효성 여부 확인

인증서는 분실, 발급자격 변동, 기간만료 등의 사유로 그 효력이 상실될 수 있으므로, 의료기관에서는 인증기관과 교신하여 해당 인증서의 유효성 여부 확인이 필요하다. 〈표 6〉은 인증서의 유효성을 검증하는 방법을 정의하였다. 각 의료기관은 기관환경에 맞는 방법을 선택하여 적용할 수 있다.

2) 전자서명의 적용시점

의료기관에서는 마취기록지, 수술기록지와 같이 연속되는 의료행위 서식이나 간호활동 기록지, 집중간호 기록지와 같이 비연속적인 의료행위 서식 등이 다양하게 사용되고 있다. 이러한 의무기록을 의료인이 전자의무기록으로 일괄하여 작성하거나 매번 작성하는 것은 의료인의 입력행태에 따른 것으로 의료인이 책임지고 판단할 사항이나, 가급적 의료인의 의료행위 시점과 전자서명 적용시점 간의 시간차이가 발생하지 않는 것이 향후 의무기록에 대한 검증시 효과적이다.

3) 인증서 발급절차 및 운영방안

인증서를 발급하기 위해서는 등록기관을 통해 사용자에 대한 신원확인 및 개인정보를 등록한다. 의료기관의 특성에 따라 등록기관을 달리 할 수 있는데, 의료기관에서 자체 등록기관

〈표 6〉 인증서 검증항목 및 내용

구 분	내 용
실시간 검증	- 해당 인증서의 유효성 확인이 필요한 시점에 매번 인증기관에 접속, 인증서 폐지목록(CRL : Certification Revocation List)을 검색하여 확인하는 방식으로, 상당한 통신량 발생 - 인터넷 뱅킹 등 실시간 유효성 확인이 반드시 필요한 업무에 적용
지정시점 검증	- 인증기관의 인증서 폐지목록(CRL)을 지정시점에 주기적(24시간 등)으로 다운로드하여 의료기관 자체 시스템에서 갱신한 상태에서 인증서에 대한 유효성을 확인 - 다음 갱신 시점까지 해당 인증서가 유효한 것으로 추정
자체 관리	- 의료기관의 경우 의료인의 근무상황을 정확히 파악할 수 있으므로 자체 프로그램에서 해당 의료인의 의료시스템 접근 여부를 제어 - 인증서 유효성 여부는 별도로 확인하지 않음.

〈표 7〉 자체 등록기관 운영의 장단점

등록기관	장 점	단 점
운영	- 인증서에 대한 즉시 조치 가능	- 인증서 관리인력 필요
미운영	- 별도의 관리인력 불필요	- 인증서에 대한 즉시 조치가 불가능하고, 인증기관에 의뢰 필요

(Registration Authority)을 운영하는 것은 다음과 같은 장단점이 있다(〈표 7〉 참조).

인증기관의 등록기관을 경유하는 인증서 발급절차는 〈그림 5〉와 같다. 사용자는 오프라인으로 등록기관에서 신원확인을 거친 후에 정보를 입력하면 그 정보는 인증기관에 저장된다. 이 정보를 통해 사용자에 대한 인증서를 발급한다.

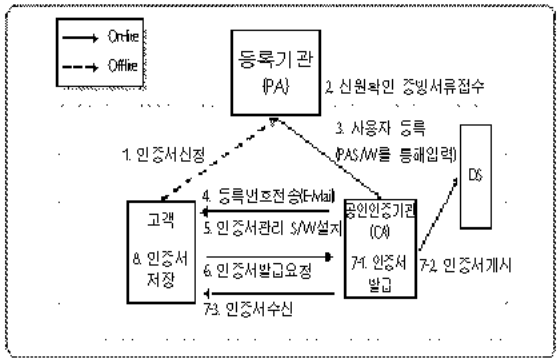
4) 개인 키 저장매체 운영방안

개인 키 저장의 안전성 및 체계적이고 일관성 있는 관리, 사용자의 이동성과 편의성 확보를 위하여 개인 키 저장매체의 지원이 요구된다.

관련문헌을 통해 〈표 8〉과 같이 저장매체의 장단점 비교를 통해 각 의료기관의 환경에 맞춰 저장매체를 결정할 필요가 있다. 안전성, 보안성, 이동성을 고려하여 스마트 카드 또는 USB Key가 상대적으로 우수하다고 할 수 있다(김형훈 2002; 탁승호 2004).

5) 무장애 · 무정지 운영방안

무장애 · 무정지 운영을 위해 전체 전자의무기록 시스템을 백업 시스템 등의 차원에서 접근할 필요가 있다.



〈그림 5〉 인증서 발급절차

〈표 8〉 인증서 저장매체의 장단점 비교

구 분	장 점	단 점
스마트카드 (인증서 저장 전용)	- 최상위 보안성 제공 - 이동형 저장매체	- 타 매체에 비해 비용과다
스마트카드 (신용카드 겸용)	- 최상위 보안성 제공 - 이동형 저장매체 - 별도의 비용이 없음.	- 신용 카드 겸용이므로 카드 신청 필요 - 신용 카드에 대한 거부감
USB Key (CPU Type)	- 최상위 보안성 제공 - 이동형 저장매체	- 타 매체에 비해 비용과다 - 적용사례 없음.
USB Key (Memory Type)	- 이동형 저장매체 - 타 이동형 저장매체 대비 비용저렴	- CPU Type과 대비 시 보안성 저하
서버 저장 방식	- 최상의 이동성 제공 - 편의성 극대화	- 보안성 취약 - 개인 키는 개인이 지배 관리하여야 하므로 개인의 동의절차 필요 - 시스템 효율성 저하 우려
하드 디스크	- 별도의 비용 없음.	- 보안성 취약 - 이동사용이 불가능

의무기록의 법정 보존기간(진료기록부 10년, 간호기록부 5년, 처방전 2년 등)은 정보기술(Information Technology) 발전주기에 비해 상당히 장기간이므로 관련 기술의 발전과 무관한 지속적인 운용성을 확보할 필요가 있다.

인증기관의 경우, 관련 법에서 요구하는 안

전성과 신뢰성 보장을 위하여 네트워크를 포함한 모든 인증 시스템을 이중화하여 운영하고 있다. 때문에 전자의무기록 시스템에 대한 안정성 및 신뢰성을 위하여 동일한 방식으로 이중화를 검토하여야 할 것이다.

6) 전자서명된 전자의무기록 데이터의 저장 방식

전자서명된 전자의무기록 데이터의 경우 DB, file, XML, PDF 등의 모든 저장형태에 대한 지원이 가능하여야 한다.

① 의료인 인사 테이블 변경 : 의료기관에서 사용하는 기존의 의료인 인사 테이블에 "현재 사용 중인 인증서 필드(1.2KB)"와 "인증서 유효성 여부(1Byte) 필드"를 추가한다(<그림 6> 참조).

② 인증서 이력관리 테이블 신설 : 의무기록의 법정 보존기간과 1년인 인증서의 유효기간이 서로 상이하므로, 인증서 이력관리 테이블을 신설하여 향후 의무기록에 대한 검증 발생시 의료인 인사 테이블과 상호 참조하여 검증한다(<그림 7> 참조).

③ 전자의무기록 데이터의 저장 : 해당 의무기록에 대한 전자서명 값만을 저장하여 전체적인 데이터베이스 사용 용량을 최소화 할 수 있도록 구성한다.

④ 시간정보 추가 : 의무기록의 경우 시간에 대한 정보가 중요하므로 전자서명을 수행하는 시간정보를 추가한다.

⑤ 전자서명 값 : 의무기록+의료인 ID+시간정보를 포함한 약 172Byte의 전자서명 값이 생성되며, 그 크기는 전자서명 원문자료의 크기와 무관하다(<그림 8> 참조).

7) 저장된 전자서명 또는 인증 데이터의 활용 방법

검찰이나 보건복지부에서 자료요청시 다음과 같이 데이터를 조합하여 제출함으로써, 의무기록에 대한 위변조 여부와 전자서명자의 확인이 가능하다(<그림 9> 참조).

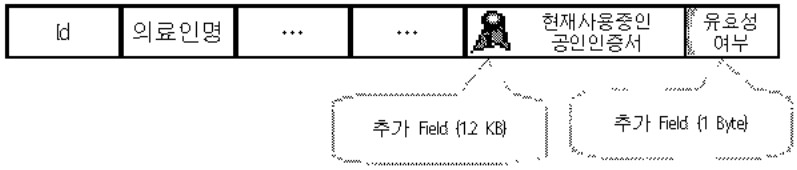
4.3 전자의무기록에 대한 전자서명 적용지침

신뢰할 수 있는 인증기관에서 발급한 인증서를 통해 전자의무기록에 대해 전자서명을 적용할 경우, 전자의무기록을 사용하는 의료인의 신원확인, 진료내용의 위·변조 방지, 진료정보의 생성에 대한 부인방지를 보증할 수 있다.

이런 전자서명의 장점을 최대한 활용하기 위해서는 각 의료기관이 전자의무기록에 대해 전자서명을 적용하기 위한 범국가적인 적용지침이 무엇보다 먼저 마련되어야 할 것이다. 이를 위해 다음과 같이 전자서명의 적용주체, 적용시점, 유효성확인 방법, 관리책임의 범위, 그리고 전자의무기록의 보관 및 관리의 기준을 제시하였다.

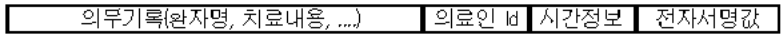
4.3.1 전자서명의 주체

전자의무기록을 최종 작성한 의료인이 전자서명을 한다. 다만, 이를 근거로 하여 원외로 교부되는 전자의무기록, 전자처방전 등에는 의료기관 개설자가 (법인)전자서명을 추가할 수

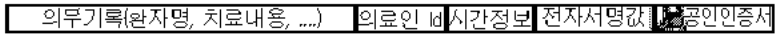


〈그림 6〉 의료인 인사 테이블

〈그림 7〉 인증서 이력관리 테이블



〈그림 8〉 인증서 이력관리 테이블



〈그림 9〉 인증서 이력관리 테이블

있다.

1) 의료인 외 의료기관 종사자의 전자서명

① 물리치료사, 사회사업사, 영양사, 작업치료사, 약사 등이 작성하는 전자의무기록에도 해당 작성자가 전자서명을 한다.

② 임상병리검사 등과 같이 실제 정보생성자(임상병리사 등)와 정보확인자(진단검사의학과장 등)가 다른 경우, 정보확인자가 전자서명을 하되, 실제 정보생성자의 전자서명은 생략할 수 있다.

③ 의무기록사는 의무기록지의 작성완료 여부에 대한 최종 확인자 역할을 수행하므로 그 근거를 기록으로 남길 필요가 있으나, 반드시 전자서명을 적용하지 않아도 무방하다.

2) 의료기관 외부로 교부시의 전제사항

의료기관 외부로 교부되는 전자의무기록, 전자처방전 등에는 이를 작성한 의료인의 전자서명이 반드시 포함되어야 한다.

3) 의료기관 외부에서 들어오는 의무기록

의료기관 외부에서 들어오는 진료의뢰서, 검사결과 등을 입력하여 전자의무기록으로 만들 경우, 그 입력내용을 최종 확인한 자가 전자서명을 한다.

4) 기존 의무기록

기존 의무기록을 전자문서화 할 경우, 원본과의 정확성을 최종 확인한 자가 전자서명한다. 다만, 의료법 시행규칙 제18조(진료에 관한 기록의 보존) 제2, 3항을 적용하는 경우에는 전자서명을 생략할 수 있다.

4.3.2 전자서명의 시점

서명자는 환자별로, 서식 또는 저장 단위별로 전자의무기록의 작성이 완료되는 시점에 전자서명을 한다.

1) 전자서명 적용 단위

서명자는 환자별로 전자서명하는 것을 기본으로 하여, 각각의 환자에 대한 서식 또는 저장 단위별로 전자서명을 한다.

2) 작성시점 관리

전자의무기록의 이력관리를 위하여 작성시점 관리를 한다.

4.3.3 인증서의 유효성 확인

의료기관은 전자의무기록에 전자서명을 하는 자의 자격을 검증하고, 최소한 일 1회 이상 인증기관과 교신하여 해당 공인인증서의 유효성을 확인한다.

1) 전자서명을 하는 자에 대한 자격검증

전자서명을 하는 자의 자격검증을 위해서는 전자서명 인증서 관리가 필요한 바, 이를 위해서는 개별 의료인 또는 의료기관 종사자의 재직상태 및 제반 자격관련 정보가 유지, 관리되어야 한다.

2) 인증서의 유효성

전자의무기록에 전자서명시 근거가 되는 인증서는 그 이용범위와 용도 등이 적합한 것이어야 한다. 의료기관에서는 인증서관리 소프트웨어를 사용하여 이를 확인할 수 있다. 인증서는 분실, 발급자격 변동, 기간만료 등의 사유로 효력이 상실될 수 있다. 따라서, 의료기관에서는 전자서명시마다 해당 인증서의 유효성을 확인해야 한다. 그러나, 이 경우에는 과도한 통신량을 유발시키므로, 의료기관에서 전자서명을 하는 자에 대한 자격검증을 실시하는 전제하에, 최소한 일 1회 이상 인증기관과 교신하여 해당 인증서의 유효성을 확인한다.

4.3.4 전자서명의 관리책임

전자서명 가입자는 자신의 전자서명 생성정보(이하 "개인 키"라 한다)를 안전하게 생성, 보관 및 관리하며, 분실 · 훼손 또는 도난 · 유출되지 않도록 적절한 조치를 취한다.

1) 전자서명 가입자의 의무

전자서명 가입자는 개인 키를 분실 · 훼손한 경우, 또는 도난 · 유출 · 훼손될 수 있는 위험을 인지한 때에는 지체 없이 그 사실을 인증기관에 통보하여 기존 인증서를 폐지하고, 신규 인증서를 발급받아 사용한다. 개인 키 저장매체는 그 소요 비용과 안정성을 고려하여 이용환경에 적합한 매체로 선정한다.

4.3.5 전자의무기록의 보관 및 관리

전자의무기록은 안전하게 관리 · 보존 되어야 하며, 이를 검증 · 확인할 수 있는 적절한 장

비 및 수단을 갖춘다.

1) 전자의무기록의 법적 보호

전자서명이 없는 전자문서는 전자의무기록으로서의 법적인 보호를 받지 못한다.

2) 안전한 관리 · 보존

전자의무기록과 그에 대한 전자서명 값 및 전자서명자가 전자서명시 근거로 한 인증서를 안전하게 관리 · 보존해야함을 말한다.

3) 검증 · 확인

검증 · 확인이라 함은 다음 사항을 말한다.

① 전자서명을 행한 전자서명자의 확인

② 전자서명이 있은 후 당해 전자의무기록의 변경여부 확인

③ 전자서명이 있은 후 당해 전자서명 값의 변경여부 확인

4) 적절한 장비 및 수단

전자서명 검증에 필요한 하드웨어(전자의무기록과 그에 대한 공인전자서명 값 및 인증서의 저장매체를 취급할 수 있는 장치 포함) 및 소프트웨어(운영환경 및 응용 소프트웨어, 공인인증서 관리 소프트웨어 포함)를 말한다.

5) 네트워크에 연결되지 아니하는 백업 저장 시스템

전자서명된 백업 전자의무기록은 적절한 저장매체에 소산 보관한다.

5. 결 론

인터넷 및 IT기술의 발달은 의료기관에도 많은 변화를 야기했다. 의무기록도 종이위주에서 전자문서의 형태로 변화하여 단순기록에서 다양한 방법으로 활용되고 있다. 때문에 국제적으로 전자의무기록에 대한 규정 및 지침을 만들어 사용을 권고하고 있다.

본 논문은 전자의무기록이 활성화되기 위해 선행되어야 할 정보보호라는 부분에 초점을 두었으며, 특히 개인정보보호라는 측면에서 전자서명을 적용하기 위해 다음과 같은 기준을 제시하였다.

1) 개인의료정보 보호방안을 수립

의료분야에서 개인의료정보의 정의, 개인의료정보의 사용공개의 원칙 및 범위, 그리고 개인의료정보에 대한 개인의 권리를 규정하였다. 이런 기준을 통해 전자의무기록 시스템을 구축하는데 있어 개인의 권리보호를 위한 최소한의 기준이 될 것이다.

2) 전자의무기록 보안에 대한 표준화를 수립

개인정보보호 및 전자의무기록의 활용이라는 두 가지의 목적을 동시에 달성하기 위해서는 전자의무기록에 대한 보안표준화가 완성되어야 한다. 때문에 본 논문에서는 보안표준화를 위하여 관련 법률을 분석하여 추가적으로 검토사항을 제시하였다. 또한 전자의무기록 시스템에 전자서명을 적용하기 위한 항목 및 세부사항을 제시하였다. 이를 통해 각 의료기관에서 전자서명을 적용하는 데 혼선을 막을 수 있을 뿐만 아니라 상호호환성을 위한 가이드라인이 될 것이다.

3) 전자의무기록에 대한 전자서명 적용지침

전자서명을 전자의무기록에 적용하기 위한 전자서명의 주체, 전자서명의 시점, 인증서의

유효성 확인, 그리고 전자서명의 관리책임에 대한 지침을 제시하였다.

이상과 같이 본 논문에서는 국가적인 차원에서 의료분야 정보보호 지침을 마련하기 위한 가이드라인을 제시하였다.

전자서명은 적용하는 것보다 유지하는 것이 더 어렵다. 본 논문에서는 보안을 강화하기 위한 전자서명 적용 가이드라인 및 적용방법을 예시하였으나, 전자서명의 신뢰성을 강화하기 위한 인증정책 및 관련 시스템 도입을 위한 가이드라인은 추후의 과제로 남겨놓았다. 때문에 완전한 정보보호 지침이 마련되기 위해서는 이러한 내용을 포함하여 포괄적인 지침이 제시되어야 할 것이다.

참고문헌

김동수. 2004. 전자의무기록의 개념 및 도입현황. 『2004년도 한국병원경영학회』, 2004년 4월 30일. (서울: 연세대학교).

김윤연. 2004. EMR 사례분석. 『2004년도 대한의료정보학회 추계학술대회』, 2004년 11월 19일. (부산: 부산대학교).

김형훈. 2002. 『USB Guide』. 서울: ohm.

이동훈. 2003. 전자서명기술. 『제8회 정보보호 심포지엄』, 2003년 7월 15일. (서울: 고려대학교).

이만영외. 1999. 『전자상거래 보안기술』. 서울: 생능출판사.

전자정부지원센터. 2004. 행정자치부 전자정부지원센터 홈페이지. (인용 2005. 2. 11). <http://www.gcc.go.kr>.

채영문. 2004. 『e Health 산업육성을 위한 정책제언』. 서울: 연세대학교.

탁승호. 2004. 『스마트카드』. 경기 : 성안당.

한림대의료원. 일송학원 홈페이지. (인용 2005. 2. 11). <http://www.gcc.go.kr>.

한국. 한국정보보호진흥원. 2004. 『PKI 기반 기술 및 국내외 기술동향 발표자료』

한국. 개인정보보호지침, 정보통신부 고시 제2002 3호.

한국. 공공기관의 개인정보보호에 관한 법률시행규칙, 총리령 제00473호.

한국. 공공기관의 개인정보보호에 관한 법률시행령, 대통령령 제18312호.

한국. 국민건강보험법, 법률 제07144호.

한국. 약사법, 법률 제07148호.

한국. 의료법, 법률 제07148호.

한국. 의료법시행규칙, 부령 제00268호.

한국. 의료법시행령, 대통령령 제18084호.

한국. 전자서명법, 법률 제06585호.

한국. 전자서명법시행규칙, 부령 제00151호.

한국. 전자서명법시행령, 대통령령 제18312호.

한국. 정보통신망이용촉진 및 정보보호 등에 관한 법률, 법률 제07142호.

한국. 정보통신망이용촉진 및 정보보호 등에 관한 법률시행규칙, 부령 제00155호.

한국. 정보통신망이용촉진 및 정보보호 등에 관한 법률시행령, 대통령령 제18505호.

한국. 정보통신부. 2004. 『민간부문의 개인정

보보호에 관한 법률(안)」, 2004. 5.

한림의료원. 한림의료원 홈페이지. [인용 2004. 12. 12]. 〈http://www.humc.hallym.or.kr/med info〉.

August 2003 Complete Privacy, Security, and Enforcement(Procedural) Regulation Text(45 CFR Parts 160 and 164), December 28, 2000 as amended May 31, 2002, August 14, 2002, February 2003, and April 17, 2003 Unofficial Version

Department of Health. 2005. *Welcome to the Department of Health*. [cited 2005. 2. 3]. 〈 http://www.dh.gov.uk/Home/fs/en〉.

DOH, UK. 2000. EHR options discussion paper

Goverment Computer Center. 정부인증관리센터 홈페이지. [인용 2005. 2. 11]. 〈www.gpki.go.kr〉.

HIPAA. 2003. HIPAA.ORG Homepage. [cited 2005. 2. 13]. 〈http://www.hipaa.org/〉.

Housley, R., W. Ford, W. Polk, and D. Solo. 1999. *Internet X.509 Public Key Infrastructure: Certificate and CRL Profile*.

IOM. 2003. *Key Capabilities of an EHR System*.

IOM. 2003. Patient Safety Achieving a New Standard for Care

J Am Med Inform Assoc. 2003. *A Proposal for EMR in U.S. Primary Care* : 1 10

KISA. 전자서명인증관리센터 홈페이지. [인용 2005. 2. 18]. 〈http://www.rootca.or.kr〉.

Medial Records Institute. 2005. Medial Records Institute Homepage. [cited 2005. 2. 10]. 〈http://www.medrecinst.com/〉.

National Academy of sciences. 2005. Institute of Medicine of the National Academy Homepage. [cited 2005. 2. 10]. 〈http://www.iom.edu/〉.

NHS Information Authority. 2002. Building the Information Core Implementing the NHS Plan.

NHSIS. 2002. *NHSIS Guidance : Executive overview of PKI and encryption certificates*.

OECD. 2001. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. [cited 2005. 2. 11]. 〈http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html〉.

Peter Waegemann. 2002. *Status Report*

2002. EHR C.

Stallings, Willam. 1999. *cryptography and network security*. London: Prentice Hall international, Inc.

U.S. DHHS, 2003. Health Insurance Reform : Security standard final rule, 2. 20.

U.S. DHHS. 1998. Security and Electronic Signature Standards proposed rule, 8. 12.

U.S. DHHS. 2002. Standard for Privacy of Individually Identifiable Health Information, Final Rule, 8. 14.

U.S. HIPAA. 1996. The Health Insurance Portability and Accountability Act.

Working draft 2.4. 2001. South Staffordshire Health Community EHR Security Policy. 10.