情 報 保 護 學 會 誌
第23卷 第4號, 2013. 8

의료부분 정보보호 관리체계 개선방안 연구

이 준 화*, 조 희 준**, 박 성 갑**, 강 윤 철**

요 약

의료부분 정보보호의 중요성이 높아감에 따라 의료정보보호 관리와 관련된 체계적인 방안이 필요하게 되었다. 이러한 체계적인 방안을 일반기업의 정보보호 관리체계(ISMS)와 역량성숙도모델통합(CMMI)을 통해 의료정보보호 관리 기준, 의료정보보호관리 프로세스, 의료정보보호관리 프로세스 성숙수준으로 구성된 의료정보보호 관리체계를 제시하였다.

Ⅰ. 서 론

1.1 연구의 필요성 및 목적

2009년 7·7 DDoS 공격, 2011년 은행 전산망 마비, 2012년 통신사 개인정보 대규모 유출 사고, 2013년 사이버 공격에서 보여지듯이 사이버 공격은 기업의 기밀이나 개인정보 등의 특정 정보를 목표로 지능화, 고도화되고 있다.

이에 기업 뿐만 아니라 의료부문에서도 정보보호가 시급하게 요구가 되었고, 기술적 대응 노력은 '일회성 관리', '부분적 보안' 등의 한계에 도달하였으며 이로 인해 '지속적 관리', '전사적 보안'을 위한 보다 높은 수준의 보안관리 활동이 가능한 의료정보보호관리 수립이 요구되었다.

또한 의료정보보호관리 수립만 아니라 더 나가 성과측정을 하여 의료정보보호 관리 성숙도 수준을 제시하고 지속적으로 발전을 추진하도록 유도해 보고자 한다.

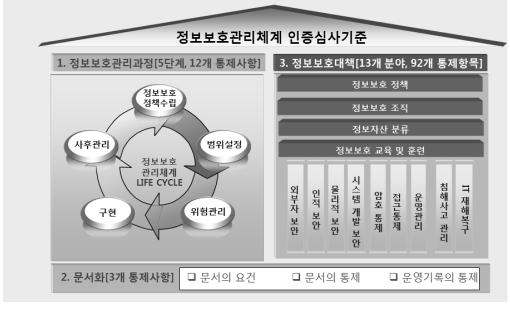
1.2 연구 참조 모델

현재 기업이 스스로 정보보호 관리체계를 구축·운영하며 활용할 수 있도록 관리체계 모델을 개발하고 인증제도를 도입하고 수행하고 있는 정보보호 관리체계(ISMS)와 조직의 사업 전담에 대한 프로세스를 평가하고 정의하여 개선해 나감으로써 수준 향상을 위한 역량성숙도모델통합(CMMi)에 대해 간략하게 살펴보면 다음과 같다.

1.2.1 정보보호 관리체계(ISMS)

기업의 경영진은 정보보호가 기업의 비즈니스 경영방침과 연계 될 수 있도록 정보보호최고책임자 지정, 전사적 정보보호정책 수립, 인력 및 예산등의 의사결정에 직접 참여할 수 있는 정보보호 관리체계의 구축하고 기업이 구축한 정보보호 관리체계의 적합성을 판단하여 인증을 부여하는 정보보호 관리체계 인증제도는 기업의 정보보호의 대한 인식 및 수준을 제고 하고 있다.

기업이 스스로 정보보호 관리체계를 구축·운영하는데 활용할 수 있도록 관리체계 모델을 개발하고 정보보호 관리체계 인증 제도를 도입하고 주요정보통신서비스



〔그림 1〕 정보보호 관리체계(ISMS) 인증 기준

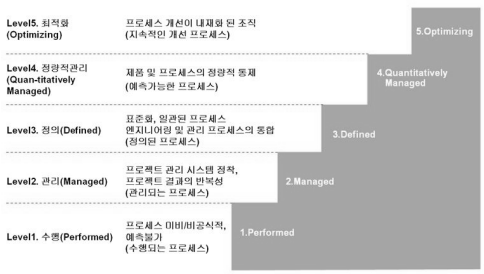
* 고려대학교 디지털경영학과(bbobbee@gmail.com)
** 고려대학교 디지털경영학과

제공자를 정보보호 관리체계 인증 제도의 인증 의무대상자로 지정하여 운영하게 되었다.

1.2.2 CMMI(역량성숙도모델통합)

서비스 및 프로세스의 개발 획득 유지보수를 위한 조직의 관리 능력을 향상시키기 위한 가이드를 제공하는데 목적이 있으며, 검증된 실무 활동을 반영하여 조직의 성숙도 및 능력 평가, 프로세스 향상을 위한 활동의 우선순위 결정, 실제 프로세스 향상을 위한 구현 활동을 지원하는 프레임워크로 구성되어 있다.

역량성숙도모델통합을 도입시에는 두 가지 방식이 있다, 하나는 단계적 방식이고, 또 하나는 연속적인 방식이다. 단계적 방식은 5단계의 성숙도별 정해진 프로세스 원칙을 지키고 각 단계마다 인증을 받은 것이다. 연속적인 방식은 프로세스 영역별로 능력 level이 0~5 단계로 정해져 있다. 각각의 프로세스 개선 활동을 프로세스 관리, 프로젝트 관리, 엔지니어링, 지원의 4개로 구분 짓고 프로세스를 선택하여 개선할 수 있다.



〔그림 2〕 역량성숙도모델통합(CMMI) 성숙도 Level

1.3 의료정보보호 관리체계 적용 방법

본 연구에서는 일반 정보보호 관리의 기준과 프로세스를 가지고 의료부분의 정보보호 관리의 기준과 프로세스를 수립하였으며, 역량성숙도모델을 참고하여 의료부분의 정보보호 관리의 지속적인 성숙도 향상을 위하여 의료정보보호 관리 성숙 수준을 포함하여 의료정보보호 관리체계를 제시하였다.

Ⅱ. 본론

2.1 의료정보보호 관리 프로세스

조직 내·외부 위협요소의 변화 또는 새로운 취약점 발견 등을 대응하기 위하여 지속적으로 유지 관리되는 순환 주기의 형태를 가진 정보보호 관리 과정에 의료부분을 추가하여 의료정보보호 관리 과정을 수립한다.

〔그림 3〕 의료정보보호 관리 프로세스

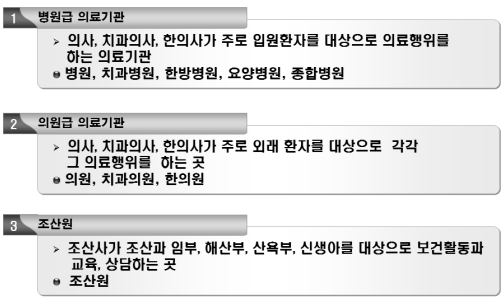
〔표 1〕 의료정보보호 관리 프로세스의 구체적인 요구사항

관리과정	요구사항	관련문서
정보보호정책 수립 및 범위설정	- 조직 전반에 걸친 상위 수준의 정보보호 정책 수립 - 정보보호 관리체계 범위 설정	- 정보보호정책서 - 정보보호 관리체계 범위서 - 정보자산 목록 - 네트워크 및 시스템구성
경영진 책임 및 조직 구성	- 정보보호를 수행하기 위한 조직 내 각 부문의 책임 설정 - 경영진 참여 가능하도록 보고 및 의사결정체계 구축	- 정보보호조직도
위험관리	- 위험관리 방법 및 계획수립 - 위험식별 및 위험도 평가 - 정보보호 대책 선정 - 구현 계획 수립	- 위험관리지침 - 위험관리 계획서 - 위험분석, 평가 보고서
정보보호대책 구현	- 정보보호 대책 구현 및 이행 확인 - 내부 공유 및 교육	- 정보보호대책 명세서 정보보호계획서 정보보호계획 이행결과 보고서
사후 관리	- 법적 요구사항 준수 검토 - 정보보호 관리체계 운영 현황 관리 - 정기적인 내부감사를 통해 정책 준수 확인	- 정보보호 관리체계 내부감사보고서 - 정보보호 관리체계 운영 현황

2.2 의료 정보보호관리 기준

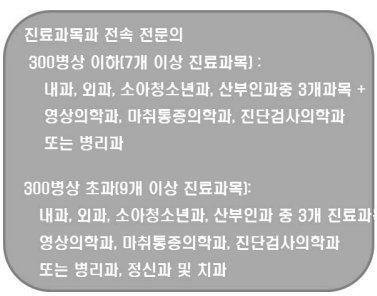
2.2.1 의료기관

의료 정보보호관리 기준은 의료기관에 따라 의료정보보호에 대한 객관적이고 대표성 있는 분류 기준이 필요하다. 의료기관 분류기준은 다음과 같다.



〔그림 4〕 의료기관 분류

종합병원의 요건 중 진료과목과 전속 전문의에 따라 300병상 이하일때는 7개이상 이고 300병상 초과 일때는 9개이상 진료과목이 되어야 한다 .



〔그림 5〕 종항병원의 요건

의료정보보호 관리의 기준은 의료기관에 적절히 맞게 항목들을 미선정할 수 있고, 미선정 항목이 있을 경우 사용을 명시하고 정보보호책임자 등 경영진의 승인을 득하여 부주의 또는 의도적으로 선정이 배제되지 않도록 한다.

2.2.2 의료 서비스

의료서비스를 내외부로 나눠어 살펴보면 내부에는 원가, 회계, 인사, 진료, 경영, 구매, 원가, 재무, 의료정보시스템, 의료장비관리, 연구 등 서비스와 외부와에 연동은 재료/물품 공급회사, 의료장비공급회사, 약국/제약회사, 보건복지부, 국민건강공단, 심사평가원, 협력병원, 환자 등 연계되어야 할 것들이 많이 있다. 이러한 서비스에 대해 중요 정보의 활용과 개인정보보호가 필요하게 된다.

신원보호서비스, 사용자 ID 관리 서비스, 접근제어 서비스, 익명화 서비스, 사용자 인증 서비스, 보안 감사 서비스, 일반 보안 서비스, 동의, 지시 관리 서비스, 암호화 서비스, 전자 서명 서비스를 고려하여 의료정보보호관리 기준을 설정해야 한다.

2.2.3 의료정보보호관리 기준

의료기관과 의료서비스를 따라 분류 기준을 만들고 기존의 정보보호관리 기준에 추가하며 그 기준을 제시하였다. 추가된 주 내용은 다음과 같은 것을 고려하여 제시한다.

의료 디지털 정보의 저장과 교류

정보가 교류, 공유되는 환경에서 환자 정보의 저장과 관리에 대한 주 책임 부여 문제, 병원의 통합이나 폐업 등의 경우에서 환자 정보의 소유권 문제, 의료정보 교환을 위한 표준화 체계 구축 부재 등

의료 디지털 정보 파기

디지털 정보의 경우 완전한 파기에 대하 확신이 어렵고 정보 파기에 대한 관한 보안 책임과 불이익을 제도적으로 명시하고 보안 감사 추적 및 문서보안 솔루션을 등을 활용

전자 서명 범위 및 주기

전자서명의 시점이나 서명 범위, 빈도 등에 대한 지정 및 이행

의료기기

의료 기기 특성상 분실이나 도난이 쉬움, 의료 기기 내부에 저장된 데이터도 함상 유실 가능성 , 높은 수준의 보안기술 정책의 제도적 수립 필요, 의료기기의 관리, 의료기기가 하나의 시스템이다.

DB정보 암호

의료정보 유실, 유출, 무단 사용 등에 방지를 위해 DB정보의 암호화 적용

보안감사로그

보안감사에 대한 대상, 항목, 횟수, 저장 기관, 로그 분석, 로그 알람 등에 대한 체계적인 보안 정책, 필수적인 보안감사 항목이나 감사 권장 주기, 저장기간, 보안감사 활동 필요

〔표 2〕 의료정보보호관리 기준인 통제분야 및 통제항목

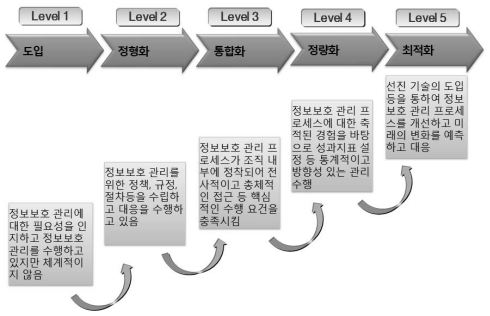
정보보호대책	통제 분야	통제항목
정보보호 정책	정책의 승인 및 공표	- 정책의 승인 - 정책의 공표
	정책의 체계	- 상위 정책과 연계성 - 정책 시행 문서 수립
	정책의 유지관리	- 정책의 검토 - 정책 문서의 관리
정보보호 조직	조직의 체계	- 정보보호 최고책임자 지정 - 실무조직 구성 - 정보보호위원회
	역할 및 책임	- 역할과 책임
외부자 보안	보안요구사항 정의	- 외부자 계약시 보안요구사항
	외부자 보안 이행	- 부자 보안 이행 관리 - 외부자 계약 만료 시 보안
정보자산 분류	정보자산 식별 및 책임	- 정보자산 식별 - 정보자산별 책임할당
	정보자산의 분류 및 취급	- 보안등급과 취급
정보보호 교육	교육 프로그램 수립	- 교육계획 - 교육 대상 - 교육 내용 및 방법
	교육시행 및 평가	- 교육 시행 및 평가
인적보안	정보보호 책임	- 주요 직무자 지정 및 감옥 - 직무 분리 - 비밀 유지서약서
	인사규정	- 퇴직 및 직무변경 관리 - 상별 규정
물리적 보안	물리적 보호구역	- 보호구역 지정 - 보호설비 - 보호구역 내 작업 - 출입통제 - 모바일기기 반출입
	시스템 보호	- 케이블보안 - 시스템배치 및 관리
	사무실보안	- 개인업무환경보안 - 공용업무 환경보안

정보보호대책	통제 분야	통제항목
시스템개발 보안	분석 및 설계 보안관리	- 보안요구사하 정의 - 인증 및 암호화 기능 - 보안로그 기능 - 접근권한 기능
	구현 및 이관 보안	- 구현 및 시험 - 개발과 운영 환경 분리 - 운영환경이관 - 시험데이터보안 - 소스 프로그램 보안
	외주개발보안	- 외주개발보안
암호토제	암호정책	- 암호 정책수립
	암호 키 관리	- 암호키 생성 및 이용
접근통제	접근통제 정책	- 접근통제 정택 수립
	접근권한 관리	- 사용자 등록 및 권한 분여 - 관리자 및 특수 권하 관리 - 접근권한 검토
	사용자 인증 및 식별	- 사용자 인증 - 사용자 식별 - 사용자 패스워드 관리 - 이용자 패스워드 관리
접근통제	접근통제	- 네트워크 적근 - 서버 접근 - 응용프로그램 접근 - 데이터베이스 접근 - 모바일 기기 접근 - 인터넷 접속 - 의료기기 접근
운영보안	운영 절차 및 변경	- 운영절차 수립 - 변경관리
	시스템 및 서비스 운영 보안	- 정보시스템 인수 - 보안시스템 운영 - 성능 및 용량관리 - 장애관리 - 원격운영관리 - 스마트워크 보안 - 무선네트워크 보안 - 의료기기 보안 - 공개서버 보안 - 백업관리 - 취약점 점검
	전자거래 및 정보전송 보안	- 전자거래 보안 - 정보전송 정책 수립 및 협약 체결
	매체 보안	- 정보시스템 저장 매체 관리 - 휴대용 저장매체 관리
	안성코드 관리	- 악성코드 통제 - 패치관리
	로그관리 및 모니터링	- 시각 동기화 - 로그기록 및 보존 - 접근 및 사용 모니터링 - 침해시도 모니터링

정보보호대책	통제 분야	통제항목
침해사고 관리	절차 및 체계	- 침해사고 대응절차 수립 - 침해사고 대응체계 구축
	대응 및 복구	- 침해사고 훈련 - 침해사고 보고 - 침해사고 처리 및 복구
	사후 관리	- 침해사고 분석 및 고유 - 재발방지
IT 재배 복구	체계 구축	- IT 재해복구 체계 구축
	대책 구현	- 영향분석에 따른 복구 대책 수립 - 시험 및 유지관리

3. 의료정보보호 관리 프로세스의 성숙 수준

의료정보보호관리 성숙수준은 조직이 수행하고 있는 정보보호관리의 체계화 정도를 나타낸다. 즉 성숙수준이 높을수록 체계적이며 지속적 정보보호가 수행되고 있음을 의미한다. 의료정보보호관리 성숙수준을 도입-정형화-통합화-정량화-최적화의 5단계로 구분한다.



〔그림 6〕 의료정보보호관리 성숙수준 5단계

성숙단계 1은 도입 단계이다.

도입단계는 의료정보보호 관리의 초기 단계로 정보보호 관리에 대한 문제점과 필요성을 부분적으로는 인지하고 있지만, 정책과 정형화된 프로세스가 미비하여 정보보호관리가 담당자 개개인의 능력에 의존해 수행되는 단계이다. 또한 기본적인 수준의 식별 및 계획이 수립되고 있으나, 전반적으로 정보보호의 사고가 발생소지가 높은 단계이다.

성숙단계 2는 정형화 단계이다.

정형화단계는 의료정보보호를 위한 정책 및 규정과 정보보호 관리와 관련된 제반 프로세스가 정형화되어 있으며, 정의된 절차에 따라 기본적인 정보보호관리가 이루어지는 단계이다 또한 정보보호 관리 상태는 취약점 및 사고에 대해 기본적인 대응이 가능하며 정보보호 기준을 정의하여 시스템 및 일부 사용하고 있는 등 기본적인 운영활동을 수행하고 있는 단계이다.

성숙단계 3은 통합화 단계이다.

통합화 단계는 전사적인 연계 및 통합 관점에서 일관성 있는 정보보호관리가 이루어지고 있으며 취약점 및 사고가 서비스되고 있는 단계이다. 정책 및 규정이 병원 전체에 반영되어 있으며, 정보보호 관리 요소간의 연계성이 확립되어 있다. 또한 침해사고, 재해 복구 등의 프로세스가 안정화돼 있으며 개선 작업이 수행되고 정보보호 관리의 제반 활동이 정성적으로 수행되고 있지만 정량화되어 측정되지는 않는 단계이다.

성숙단계 4은 정량화 단계이다.

정량화 단계는 정량적인 방법을 통해 지속적·안정적으로 정보보호 관리 제반 활동을 관리하며, 목표 달성 여부를 측정·확인하는 단계이다.

성숙단계 5는 최적화 단계이다.

최적화 단계는 정보보호 프로세스의 개선상항을 지속적으로 도출하고 실행하며 평가를 통해 사후 관리를 수행하는 단계로, 현재의 관점에서 최적화뿐 아니라 지속적인 개선 노력을 통하여 미래의 환경 변화에 유연하게 대처할 수 있는 수준이다.

의료정보보호 관리 성숙수준은 수준진단 항목별로 측정한다. 성숙수준의 측정방법은 병원 기준에 따라 상이한데. 이것은 기준별로 정보보호에 영향을 주는 관련 프로세스가 서로 다르기 때문이다.

〔표 3〕 의료정보보호 관리체계 성숙 수준 진단 항목

구분	진단항목	설명
의료정보자산 관리	정보자산 목록관리	의료정보자산 모록 식별
	네트워크 구성도 관리	네크워크 구성도를 최신으로 유지
	정보자산 관리 책임	의료정보자산의 대한 책임자와 담당자를 지정
서버보안	접근권한 관리	의료정보시스템 계정 및 접근권한 현황을 주기적으로 검토
	패스워드 관리	추측하기 어렵도록 설정하고 주기적으로 변경 관리
	접근기록 모니터링	접속로그를 자동 기록 주지적인 검토를 수행
	접근제어	인가받은 사용자만이 접근가능하도록 접근통제
	보안패치 관리	정기적인 패치, 긴급패치 등의 절차 및 이행
	백업계획 수립 및 수행, 복구점검	백업이행, 백업매체의 안전한 보관 관리, 복구점검 수행
	의료정보시스템 취약점 점검 계획 수립 수행	의료정보시스템 취약점 점검 계획 수립 및 수행
	의료정보시스템취약점 조치 및 결과보고	취약점 점검 결과 조치 및 이행여부 확인
네트워크 보안	서버스 구성관리	의료정보시스템을 분리 구성하고 안전한 구성대책을 시행
	네트워크 이상징후 탐지 및 보고	실시간 탐지하고 다양한 보안위협에 대한 보고 및 정책 적용
	네트워크장비 접근규칙 주기적 검토	접근규칙을 적용하고 주기적인 검토
	네트워크 보안 강화	적절한 보안 시스템을 설치, 활성화하여 운영
정보보호 의료 시스템 관리	정보보호시스템접근규칙 쟌리 절차	접근규칙의 생성, 변경, 삭제 시에 요청, 검토, 승인등의 절차 시행
	정보보호시스템접근규칙 주기적 검토	주기적인 접근규칙 적절성 검토를 수행하여 기록, 보관하고 검토결과를 보고
	정보보호시스템 접근통제	관리접근이 안전한 네트워크 통신을 통제
의료응용 SW 보안	어플리케이션 접근권한 검토	어플리케이션에 대한 관리자 및 사용자 권한을 주기적으로 검토
	어플리케이션 접근권한 기록 보관	직무변경 시 접근권한을 삭제, 기록을 주기적으로 검토
	어플리케이션 패스워드 관리	어플리케이션 관리자 및 사용자 사용규칙을 적용 저장 시 암호화
	저장시 암호화 대책	중요정보의 DB 저장 시에 암호화 대상 방법 등의 암호화 대책 수립
	전송 시 암호화 대책	중요정보의 전송을 위한 암호화 대책을 수립
	접근기록 및 보관상태 점검	접근기록을 자동 기록, 보관하고 이를 주기적으로 점검
	웹취약점 점검	취약점 점검 계획을 수립 및 시행
	웹취약점 개선	점검 결과와 발견된 취약점을 조치
	DBMS 취약점 점검	DBMS에 대한 취약점 점검 계획을 수립 및 시행
	소스프로그램 보안	소스프로그램 전전을 관리하고 소스 관련장소에 물리적 접근통제
	이용자보호기능 제공	키보드보안프로그램, 패스워드 규칙 적용
운영지침	운영지침 수립 및 운영	운영지침을 수립하여 시행
외부용역관리	외주용역사업 보안관리	외주용역사업의 준비 및 착수단계, 수행단계에서 보안통제 대책 수립
	주요시설의 출입통제	인가된 사람만 접근할수 있도록 CCTV 접근통제
개발 환경 보안	개발과 운영환경의 분리	개발 및 시험하는 시스템 환경과 운영 환경을 분리
	개발·테스트 환경의 보안	개발 및 테스트 시스템에 대한 접근통제
침해 대응 및 재해 복구	침해사고 대응절차	침해하고에 대한 대응조직, 대응 절차 등을 포함하는 대응대책을 수립
	침해위협대응	보안위협에 대해 조치계획 수립 및 수행
	보안관제 실시	이상징후 탐지 및 침해사고 대응을 위해 보안관제를 실시
	복구대책의 수립	재난, 재해복구대책을 수립 시행
정보보호 조직 및 교육	정보보호 담당조직·인력 구성	정보보호 전담조직·인력이 구성, 책임과 역할이 정의
	정보보호 담당인력 보안교육	담당자 연간 정보호보 교육 실시
	담당자 보안교육	정보보호교육을 년 1회이상 실시 및 검토

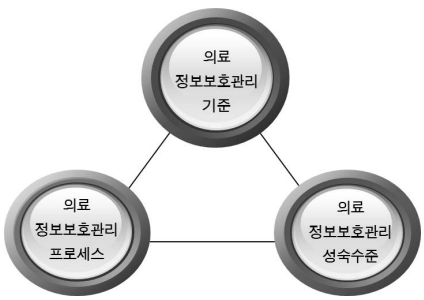
Ⅲ. 결론 및 향후 연구 과제

의료정보보호 관리의 문제를 해결하기 위해서 현재의 의료정보보호관리 수준을 정확하게 인식해야 한다. 수준이 파악되어야만 이로 인한 문제점과 원인을 정확하게 분석할 수 있고 대응 방안도 마련할 수 있다. 따라서 의료정보보호 관리체계는 의료정보보호관리 기준, 의료정보보호관리 프로세스, 의료정보보호관리 프로세스의 성숙수준과 같이 세 가지 중심축을 기본으로 하여 이루어진다.

첫 번째는 의료정보보호 관리의 대한 기준이다. 일반 기업에 사용되는 정보보호 관리체계(ISMS)를 바탕으로 의료 부문의 맞는 의료정보보호관리 기준을 제시한다.

두 번째는 의료정보보호관리 프로세스이다. 기준의 의료정보보호를 향상시키기 위해서 필요한 프로세스를 식별과 프로세스간의 연관관계로 이루어진다.

세 번째는 의료정보보호관리 프로세스의 성숙수준이다. 의료정보보호관리 프로세스의 성숙수준이 높을수록 체계적이고 정교한 관리가 수행되는 것이고 해당 의료정보보호관리 기준도 높게 유지한다.



〔그림 6〕 의료정보보호 관리체계

의료정보보호 관리체계는 의료정보보호관리 향상을 위해서 어떤 프로세스를 어떻게 개선해야 하는지에 대한 방향을 제시할 수 있도록 되어 있다. 또한 의료기관에 인식에 따라 선별적으로 적용할 수 있는 구조를 갖추고 있다. 중요도 및 위험에 따라 단계적이고 지속적인 계획을 수립하여 향상에 할용 할 수 있다.

향후 연구과제에서는 제시한 의료정보보호 관리체계를 바탕으로 병원급 의료기관, 의원급 의료기관 등 사례연구를 진행할 것이고 사례연구를 통해 의료기관에 따라 적절하게 적용될 것으로 기대한다.

참고문헌

[1] 미래창조과학부, “정보통신망 이용촉진 및 정보보호 등에 관한 법률”, March 2013
[2] 보건복지부, “의료법”, January 2013
[3] 식품의약품안전처, “의료기기법”, March 2013
[4] 미래창조과학부 “정보보호 관리체계 인증제도 안내서”, March 2013.
[5] 한국정보보호진흥원 “정보보호 관리체계 인증 모범사례,” December 2008.
[6] 한국정보보호진흥원 ‘ISMS인제 제도 소개“, http://isms.kisa.or.kr/kor/main.jsp
[7] ISACA, COBIT 4.1, 2008,www.isaca.org
[8] ISO/IEC27001:2005 Requirement
[9] 조희준, IT 거버넌스 프레임워크 코빗 - COBIT 4.1을 중심으로, 인포더북스, 2010.
[10] “CMMI: Capability Maturity Model Integration for System Engineering, Software Engineering, Integrated Product and Process Development and Supplier Sourcing”, March, 2002
[11] Capability Maturity Model Integration (CMMI) Version 1.1 (CMMI-SE/ SW/ IPPD/ SS. V1.1) Staged Representation CMU/SEI-2002-TR-011. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA

〈著者紹介〉

이 준 화 (LEE JUN HWA)
1997년 2월 : 명지대학교 전자공학과 졸업
1999년 2월 : 명지대학교 전자공학과 석사
2013년 9월 : 고려대학교 디지털경영학과 박사과정 예정
<관심분야> 의료 IT 거버넌스 및 정보보호 거버넌스, 의료 IT감사, 내부통제, ISMS(정보보호관리체계), PIMS(개인정보관리체계), IT-SM(IT서비스관리체계), BCMS(비지니스연속성관리체계), 디지털 포렌식, 의료 포렌식, 빅데이터 등