TTA Technical Report

기술보고서

TTAR-xx.xxxx

제정일: 2019년 12월 xx일

디지털병원 정보보호 지침 -
제1부: 사이버보안 행동강령(기술보고서)

Guidance of Digital Hospital Security
Part I : Cybersecurity Code of Practice
(Technical Report)

한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회 바이오 인식 프로젝트그룹(PG505)

기술보고서안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
기술보고서(과제) 제안	한근희	건국대학교	교수	PG505 특별위원	TTAR-xx.xxxx
	김동원	건양대학교	교수	-	
기술보고서 작성자	한근희	건국대학교	교수	PG505 특별위원	TTAR-xx.xxxx
	김동원	건양대학교	교수	-	
사무국 담당	김재웅	TTA	단장	사무국	
	문서연	TTA	선임	사무국	

본 기술보고서 발간 이전에 접수된 지식재산권 확약서 정보는 본 기술보고서의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 기술보고서와 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109

발행일 : 2019.10

서 문

1 기술보고서의 목적

본 기술보고서는 의료정보를 디지털화하여 저장하고 활용하는 의료기관에서 필요한 관리적, 물리적, 기술적 정보보호 요구사항을 정의한다.

2 주요 내용 요약

본 기술보고서는 의료기관에서 정보통신기술 (ICT, Information Communication Technology)을 기반으로 하는 의료정보시스템, 의료기관에서 사용하고 있는 여러 의료기기에서 세트로 동작하는 ICT 기기들과 관련 소프트웨어, 의료기관을 방문하는 자(외래, 입원, 응급, 건강검진 등)의 개인건강정보, 의료 관련 정보 등을 안전하게 보호하고, 의료 관련 종사자가 지켜야 할 제반 정보보호(개인정보보호 포함) 준수사항을 가이드하기 위해 의료 보안 관련 국제표준 기술, 미국 NIST 사이버보안 프레임워크, NIST 표준 특별보고서(SP), 산업 표준 간의 보안 통제 항목을 비교하여 제공한다.

각각의 일반적인 보안 특성을 구체적이고 다중적인 보안 통제와 비교함으로써, 특징을 좀 더 세분화하여 정의하며 이러한 특징을 실행하는데 필수적인 조치를 이해하고자 한다. 이러한 비교를 통해 얻을 수 있는 혜택 중 하나는 보안적 특정으로부터 보안 통제의 평가로까지의 추적 가능성이다.

3 인용 기술보고서와의 비교

해당사항 없음

Preface

1 Purpose

The purpose of this Technical Report is to define the administrative, physical, and technical information protection requirements needed by medical institutions to digitize, store and utilize medical information.

2 Summary

This technical report is intended for medical information systems based on ICT (Information Communication Technology) in medical institutions, ICT devices operating in various medical devices used by medical institutions, related software, (Including personal information protection), NIST cyber security framework, related NIST standards, and other related information that healthcare workers must observe, as well as personal health information, medical information, Compare the components between industry standards and best practices.

By comparing each generic security characteristic with specific and multiple security regulations, we want to define the features more granularly and understand the measures necessary to implement them. One of the benefits of these comparisons is traceability from the security specification to the evaluation of security regulations.

3 Comparison with Reference Standards

None

목 차

디지털병원 정보보호 지침 - 제1부: 사이버보안 행동강령(기술보고서)
Guidance of Digital Hospital Security - Part I : Cybersecurity Code of Practice (Technical Report)

1 적용 범위

본 기술보고서는 의료정보를 디지털화하여 저장하는 의료기관에서 지켜야 할 정보보호 및 개인정보보호 요구사항을 정의한다. 본 기술보고서 Part Ⅰ은 표준과 규제간의 비교로 유익참조, 표준, 행동 강령를 기술한다. 본 기술보고서은 모듈형이며 전체 또는 부분적으로 사용 될 수 있다.

본 기술보고서은 총 5권으로 구성되어 있다.

- Part Ⅰ: 디지털병원 정보보호지침 - 사이버보안 행동강령(Code of practice)
- Part Ⅱ: 디지털병원 정보보호지침 - 보안위협 모델링
- Part Ⅲ: 디지털병원 정보보호지침 - 의료정보시스템 정보보호 요구사항
- Part Ⅳ: 디지털병원 정보보호지침 - 의료기기 정보보호 요구사항
- Part Ⅴ: 디지털병원 정보보호지침 - 위험관리 가이드라인

2 인용 표준

해당사항 없음

3 용어정의

3.1. 디지털 병원 용어

디지털병원 정보보호 요구사항 표준을 참조한다.

3.2. 정보보호 용어

3.2.1. 책임 추적성(Accountability)

시스템 내의 각 개인은 유일하게 식별되어야 한다는 정보 보호 원칙.
이 원칙에 따라 정보 처리 시스템은 누가, 언제, 어떠한 행동을 하였는지 기록하여

필요시 그 행위자를 추적할 수 있게 하여 정보 보호 규칙을 위반한 개인을 추적할 수 있고, 각 개인은 자신의 행위에 대해서 책임을 진다.

3.2.2. 인증(Authentication)

인증은 한 개인을 식별하는 보안 절차를 의미
이 과정에서 개인은 자신이 누구라고 주장하도록 보장하지만 개인의 접근 권한에는 영향을 미치지 않는다. 사용자 이름, 패스워드 및 생체측정 스캐닝 등은 모두 인증 기술들
인증에는 크게 두 가지가 있다.

1. 사용자/과정/장치 인증보안 시스템에서는 모든 사용자들이 다른 시스템 작동을 수행하기 전에 스스로를 식별하도록 요구한다. 인증은 접근을 시도하는 사용자를 검증하는 과정. 사용자 인증의 일차적 방법은 다음과 같다.
   1) 접근 패스워드(사용자가 알고 있는 것)
   2) 접근 토큰(사용자가 소유하고 있는 것)
   3) 생체측정(지문, 손금 또는 음문 등 사용자에게 존재하는 것)
   4) 지리(위치) (특정 워크스테이션 등)
2. 데이터 인증
   데이터의 무결성이 위험에 노출되지 않았음을 검증하는 과정

3.2.3. 권한 부여 혹은 인가(Authorization)

사용자에게 무엇을 할 수 있거나, 가질 수 있는 권한을 부여하는 과정
다중 사용자 컴퓨터 시스템에서, 관리자는 어떠한 사용자가 그 시스템을 접근할 수 있는지, 그리고 부여된 사용권한의 범위(파일 디렉토리의 접근 범위, 허용된 액세스 시간, 할당된 저장 공간의 크기 등)에 대해 정의
특정 사용자가 컴퓨터 운영 시스템이나 응용프로그램에 접근 했을 때, 그 시스템이나 응용프로그램은 그 세션 동안 사용자에게 어떤 자원의 권한을 허락해야 하는지 확인 authorization은 관리자가 사용자에 대해 미리 설정 해 놓는 권한 및 사용자가 접근 할 시에 사용자의 권한 정도를 확인하는 것 모두를 지칭
논리적으로 인증은 권한부여에 우선

3.2.4. 가용성(Availability)

정보 보안의 네 가지 기본 요구 사항 중 하나인 가용성은 인가를 받은 사용자가 정보나 서비스를 요구할 경우, 정보시스템에 대한 사용 가능 여부에 대한 요구 사항 가용성의 유지는 보안 시스템의 주요 기능 중 하나. (참고: 책임추적성, 기밀성, 무결성)

3.2.4. 기밀성(Confidentiality)

정보가 유출되거나 노출되더라도 읽어 볼 수 없도록 데이터를 보호하는 것으로 권한 없는 개인, 단체 또는 프로세스에 정보를 공개하지 않도록 하는 속성
인가되지 않은 방식으로 정보를 획득할 수 없도록 하는 것으로, 정보의 기밀을 유지하는 것은 정보 보안 요구 사항의 네 가지 기본 사항 중 하나로써 프라이버시와 거의 동일 데이터의 기밀성이 지켜지지 못한 경우 위험에 노출되었다고 말한다.

3.2.6. 자료 무결성(data integrity)

변경할 수 없도록 정확성과 일관성을 유지하고 보증하는 것
데이터 무결성은 네트워크 관리자만의 서버 접근, 전송 선로 관리, 사용자 인증 수준 등 여러 가지 관리 대책이 필요
종류는 개체 무결성(Entity integrity), 영역 무결성(Domain integrity), 참조 무결성(Referential integrity) 등

3.2.7. 식별(Identification)

사람이나 객체의 유일성을 확인하는 절차, 또는 사용자 식별 부호(ID).
식별, 신원 증명, 신원 확인 등의 뜻으로, 패스워드와 함께 다수의 사용자가 이용하는 컴퓨터 시스템이나 통신망에서 정당한 사용자임을 인증 받는 절차의 필수요소
사용자의 신원확인을 위해서는 내부의 객체에 대한 접근을 시도하는 사용자를 식별(identification)하고, 인증(authentication)하게 되는데, 이때 식별은 ID의 입력을 통하여 사용자 자신이 다른 사람과 중복되지 않는 유일함을 확인하는 과정이며, 인증은 패스워드 입력을 통하여 그 사용자가 등록되어 있는 정당한 사용자인지를 확인하는 과정이 한다. 일반적으로 ID는 15자 이내의 영문자나 숫자를 조합한 문자열로 다른 사용자와 중복되지 않도록 하여 사용자 자신이 선정한다. 서비스 제공자의 망에 접속할 때는 ID와 함께 패스워드도 입력해야 한다. 서비스 제공자의 주 컴퓨터는 입력된 ID와 패스워드를 확인하여 그것이 이미 등록되어 있는 것과 일치하면 접속을 허가하게 한다. ID는 타인에게 알려져도 문제가 없지만, 패스워드가 알려지면 타인이 무단으로 서비스를 이용할 우려가 있으므로 잘 관리해야 하며, 변경이 가능하다. 게시판 등에서는 ID 대신 별명을 사용하여 ID의 무분별한 공개를 피하기도 한다.

3.2.8. 식별자(ID, Identifier)

① 데이터 항목에 이름을 부여하여 일시적으로 규정하거나, 그 데이터의 어떤 특성을 표시하기 위해서 사용하는 기호 또는 기호의 집합
② 이름을 붙이거나, 지시하거나, 위치를 나타내는 데 사용하는 부호. 데이터 구조, 데이터 항목, 프로그램 위치 등에 관련한다.
③ 자료 항목을 식별하거나 이름 붙이는 데, 또는 그 데이터의 특정 성질을 나타내는 데 사용하는 문자나 문자의 집합

3.2.9. 무결성(Integrity)

데이터 및 네트워크 보안에서 특정 정보가 인가된 사람만이 접근 또는 변경이 가능하고 데이터 전송 시 타인에 의해 해당 데이터가 위변조 되지 않았다는 것을 보장하는 것
일반적으로 데이터 무결성 보호는 인가된 관리자만의 서버 접근, 전송 선로 관리, 서지 및 전자적 충격으로부터의 하드웨어 및 저장 장치의 보호, 전송 정보의 변경 검출 메커니즘 등을 통해 이루어진다. 사용자 인증 수준 유지, 시스템 관리 절차, 유지 보수 지침 문서화, 장애 및 외부 공격에 대비한 복구 대책 수립 등 관리 대책과 적절한 무결성 보장 메커니즘 등의 기술적 대책이 필요하다.

3.2.10. 사생활 보호(Privacy)

개인의 생활이나 사건에 다른 개인의 침입이 없는 상태로, 보통 침입의 결과로는 개인 자료를 부당하거나 불법으로 수집·사용하는 것

3.2.11. 정보보호 및 개인정보보호 정책(Security & Privacy Policy)

정보보호 및 개인정보보호 등을 위해 사용되는 계획이나 과정

3.2.12. 개인정보(Personal Information)

살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)
정보 사회를 맞이하여 사회 각 분야에서 개인 정보를 널리 쓰면서 개인 정보 유출에 따른 피해가 커지고 있어, 정부는 2011년 개인정보보호법을 제정

4. 행동 강령에 적용된 국제표준 및 사실표준

사용 사례의 구조적 범위 설정을 위하여, 사이버보안 프레임워크, 관련 NIST 표준, 산업 표준 및 모범 사례(Code of Practice)간의 구성요소를 비교한다. 이러한 비교를 통해, 본 기술보고서에서 제시되는 해결책이 다루고자 하는 보안 특성 및 행동 강령 대해 기술한다. 검토된 특성은 연방 정보 시스템과 기관을 위한 보안 및 프라이버시 규제를 명시하는 NIST 특별 출판물 800-53과 국제표준기관(ISO), 국제전기표준위원회(IEC)의 정보 기술 - 보안 기술 - 정보 보안 관리를 위한 규약(ISO/IEC 27002), 국제전기표준위원회(IEC)의 정보 기술 - 보안 기술 - 의료정보 보안 관리를 위한 규약(ISO/IEC 27799), SANS 연구소의 주요 보안 통제, 1996년에 제정된 HIPPA 주요 보안 통제, Health Level Seven international(HL7) 주요 보안 통제와 대조하여 비교한다.

각각의 일반적인 보안 특성을 구체적이고 다중적인 보안 통제와 비교함으로써, 특징을 좀 더 세분화하여 정의하며 이러한 특징을 실행하는데 필수적인 조치를 이해하고자 한다. 이러한 비교를 통해 얻을 수 있는 혜택 중 하나는 보안적 특정으로부터 보안 통제의 평가로까지의 추적 가능성이다. 본 기술보고서의 “디지털병원 사이버보안 행동 강령”를 통해 디지털병원의 정보보호 요구사항에 대한 안내(guide)를 제공한다.

본 행동 강령는 다음의 표준을 인용하였다.

4.1 NIST 사이버보안 프레임워크 - CYBERSECURITY FRAMEWORK v1.1

미 대통령이 발표한 “국가 주요 기반시설의 사이버위협 대응 강화를 위한 행정명령(Improving Cirtical Infrastructure Cybersecurity Executive Order 13636)”의 일환으로 미 상무부의 국립 표준 기술 연구소(National Insitute of Standards and Technology, NIST)는 2014년 2월 국가금융·에너지·의료 및 기타 주용 시스템 제공기관이 기관의 정보와 물리적 자산을 사이버 공격으로부터 보호할 수 있도록 사이버보안 인프라의 중요한 개선을 위한 프레임워크(Framework for improving Critical Infrastructure Cybersecurity)를 발표하였다. 또한 2018년 4월 16일 1.1버전을 발표하였다. 사이버보안 프레임워크는 표준, 지침 및 관행을 정리하여 사이버보안의 여러 접근법에 대한 공통의 조직 구조를 제공한다.

4.2 NIST SP 800-53 Rev.5(DRAFT) - Security and Privacy Controls for Information Systems and Organizations

미 연방정부 행정기관의 정보시스템에 대한 보안 통제항목을 구체화하고 이를 지정하기 위한 지침이다. 정보시스템 및 그 정보의 기밀성, 무결성, 가용성을 보장하기 위해 해당 정보시스템에 설치되어나 운영되는 관리적, 운영적, 기술적 세이프가드나 대응책을 제시한다. 즉, 연방정보보안관리법 및 관련 지침이 규정하는 적정한 수준의 보안상태(adequate security)를 모든 연방정부기관에 실현하는 것이 궁극적 목표이다. 따라서 각 기관의 정보보호

프로그램과 병행 및 이에 포함되어 실시되어야 그 효율을 극대화 할 수 있다. SPO 800-53은 연방정부의 정보시스템에 대한 보안 통제항목을 구체화하고 이를 지정하기 위한 지침이다. 미 연방정부의 각 기관의 보안통제항목은 SP 800-53을 참고해 수립한다. SP 800-53은 최소한의 가장 기본적인 보안통제항목만을 포함하고 있으므로, 각 기관은 기관의 특성을 고려한 보안 관리정책을 각자 수립해야 한다.

4.3 IEC/ISO 27002:2013 - Information technology — Security techniques — Code of practice for information security controls (second edition)

ISO/IEC 27002는 최고의 정보 보안 관리 방법을 위한 지침을 제공하는 국제규격이다. 이러한 관리 방법은 조직이 조직 간 활동에 대한 확신을 쌓고 정책, 프로세스, 조직 구조 및 소프트웨어 및 하드웨어 기능을 포함하는 적절한 제어를 구현하는 데 도움이 될 것이다. 이 표준은 정보 보안 관리 시스템 구현 과정에서 통제를 선택하기 위한 참고 자료로 사용되는 일반적인 문서이다. ISO / IEC 27002는 공공 및 민간 부문, 상업 및 비영리 기관 및 정보 보안 위험에 직면한 기타 조직을 포함한 모든 유형의 조직에서 사용하기 위한 것이다.

4.4 ISO 27799:2016 - Health informatics -- Information security management in health using ISO/IEC 27002

ISO에 의해 개발된 정보보안표준으로서 의료기관 및 개인건강 주체인 개인에게 ISO/IEC 27002의 구현을 통하여 어떻게 이러한 정보들을 보호할 수 있는지 가이드를 제공하는 것이다. 11개 정보보호 대책, 39개 보안통제항목에 대한 의료정보보호관리체계 구축을 위한 요구사항을 제시하고 있다.

4.5 HIPPA 2017 - Health Insurance Portability and Accountability Act

HIPAA(Health Insurance Portability and Accountability Act)는 미국 환자의 의료정보에 대한 프라이버시권 강화를 위해 의료정보와 같은 민감한 개인정보가 적절한 프라이버시 보호책이 없이 공개되지 않을 수 있도록 하는 의료정보의 비밀보장에 관한 법률로서 대표적인 것이다. HIPAA의 보안규칙은 데이터 무결성, 기밀성 및 가용성을 보호하기 위해 관리적, 물리적, 기술적 보안대책으로 분류한다. 보안규칙은 18개의 HIPAA 표준과 36개의 구현사양이 포함되어 있다.

4.6 IHE - Integrating the Healthcare Enterprise

IHE는 컴퓨터 시스템이 정보를 공유하는 방법을 개선하기 위해 의료업계에 의해 주도권을 후원하고 있다. IHE는 방사선학자와 정보 기술(IT) 전문가들로 구성된 컨소시엄에 의해 1998 년에 설립되었다. 대한민국은 IHE를 의료정보시스템 통합으로 언급되었다. IHE는 의료 IT 시스템의 상호연동능력이 개선될 수 있도록 하는 프로세스가 동작한다. 진료정보교류 등을 위한 표준은 IHE를 중심으로 구현되고 있다.

4.7 HL7 - Health Level Seven

Health Level7(이하 HL7)의 정보 인프라 기능은 의료서비스 제공에 관여하지 않지만, 업무의 효율성과 상호 운용성을 위한 최소한의 기준 뿐만 아니라 환자의 안전, 개인정보보호 및 정보 보안을 위해 필요한 보장을 제공하는지 확인하기 위해 필요하다. HL7에서는 보안과 관련된 IN.1 Security와 IN.2 Health Record Information and Management 중 보안과 관련된 인증 요건이 포함되어 있다. IN.1 Security는 엔티티의 인증, 권한, 접근통제, 사용자 정보접근, 부인방지, 데이터 교환 보호, 데이터 라우팅 보호, 정보 서명, 그리고 환자의 프라이버시와 기밀성에 대한 내용으로 구성되어 있다. IN.2 Health Record Information and Management는 보안과 관련된 데이터의 유지, 가용성, 파괴 및 감사 기록에 대한 내용으로 구성되어 있다.

5. 행동 강령에 대한 보안 특성과 보안 통제

사용 사례의 구조적 범위 설정을 위하여, 미국 사이버보안 프레임워크, NIST 표준, 산업 표준 및 Code of Practice간의 구성요소를 비교한다. 이러한 비교를 통해, 본 기술보고서에서 제시되는 해결책이 다루고자 하는 보안 특성에 대해 기술한다. 검토된 특성은 연방 정보 시스템과 기관을 위한 보안 및 프라이버시 규제를 명시하는 NIST SP 800-53 rev.4 와 국제표준기구(ISO)/국제전기표준위원회(IEC)의 정보 기술 - 보안 기술 - 정보 보안 관리를 위한 Code of Practice(ISO/IEC 27002), ISO/IEC의 정보 기술 - 보안 기술 - 의료정보 보안 관리를 위한 Code of Practice(ISO/IEC 27799), SANS 연구소의 주요 보안 통제, HIPPA 주요 보안 통제, Health Level Seven(HL7) 주요 보안 통제와 비교하였다.

각각의 일반적인 보안 특성을 구체적이고 다중적인 보안 통제와 비교함으로써, 특징을 좀 더 세분화하여 정의하며 이러한 특징을 실행하는데 필수적인 조치 항목을 제공하고자 한다. 이러한 비교를 통해 얻을 수 있는 혜택 중 하나는 보안적 특징으로부터 보안 통제의 평가로까지의 추적 가능성이다.

<표 5-1> 의료 분야 사이버 보안 표준 간의 보안 특성 비교

보안 특징	사이버 보안 표준 및 Code of Practice					HIPAA 요구사항	HL7 요구사항
	NIST CSF	NIST 800-53 rev4	IEC/ISO 27002	IEC/ISO 27799	SANS CAG 20		
접근 통제	PR.AC-1: 신원 및 권한은 허가 받은 기기 와 사용자를 위해 관리한다.	AC-2 IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3		CSC-9	§164.312 (a)	

	PR.AC-3: 원격 접근은 관리된다	AC-17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2		CSC-17	§164.312 (a)	
	PR.AC-4: 접근 허가는 최소한의 혜택 및 분리된 책임에 관한 원칙이 적용되어 관리한다.	AC-2, AC-3, AC-5, AC-6, AC-16	6.1.3, 7.2.2, 8.1.1, 8.3.3, 10.1.3, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2, 12.4.3, 15.2.1		CSC-9	§164.312 (a)	
감사 / 모니터링	DE.CM-1: 네트워크는 잠재적인 사이버 보안 사건을 감지하기 위해 모니터링 한다.	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7 SI-4	6.1.8, 6.2.1, 8.3.3, 10.1.1, 10.1.2, 10.3.1, 10.3.2, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.4, 11.4.5, 11.4.6, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2		CSC-2, CSC-3, CSC-5, CSC-6, CSC-11	§164.312 (b)	
	DE.CM - 3 : 인적 활동은 잠재적인 사이버보안 사건을 감지하기 위해 모니터링 한다	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	6.1.8, 8.3.3, 10.10.1, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 15.2.2		CSC-6, CSC-11	§164.312 (b)	

	DE.CM-4: 악성 코드는 검출한다.	SI-3	10.4.1		CSC-7	§164.312 (b)	
	DE.CM-5: 허가되지 않은 모바일 코드는 감지한다.	SC-18, SI-4. SC-44	10.4.2, 10.10.2, 13.1.1, 13.1.2		CSC-5, CSC-6	§164.312 (b)	
	DE.CM-6: 외부 서비스 제공자 활동은 잠재적인 사이버보안 사건을 감지하기 위해 모니터링 한다.	CA-7, PS-7, SA-4, SA-9, SI-4	6.1.8, 6.1.5, 6.2.1, 6.2.3, 8.1.1, 8.1.3, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 10.10.2, 12.1.1, 12.5.5, 13.1.1, 13.1.2, 15.2.1, 15.2.2		CSC-5, CSC-6, CSC-7	§164.312 (b)	
	DE.CM-7: 허가되지 않은 사용자, 연결, 기기 및 소프트웨어에 대한 모니터링은 행해진다.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	6.1.8, 7.1.1, 7.1.2, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 10.1.1, 10.1.2, 10.3.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 11.3.2, 11.4.4, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2		CSC-1, CSC-2, CSC-5, CSC-6, CSC-7	§164.312 (b)	
	DE.CM-8: 취약성에 대한 스캔이 행해진다.	RA-5	12.6.1, 15.2.2		CSC-7, CSC-10	§164.312 (b)	
기기 무결성	PR.AC -3: 원격 접근은 관리한다.	AC-17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2		CSC-5, CSC-6, CSC-8, CSC-14	§164.312 (c), §164.308 (a)(5)(ii)(B)	

	PR.DS-1: 데이터는 보호한다.	SC-28	해당사항 없음		CSC-15	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)	
	PR.DS-3: 자원은 공식적으로 제거, 전송, 폐기를 통해 관리한다.	CM-8, MP-6, PE-16	7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3		CSC-1, CSC-2	§164.312 (c), §164.308 (a)(5)(ii)(B)	
	PR.DS-6: 무결성 검사는 소프트웨어, 펌웨어 및 정보 무결성을 증명하기 위해 사용한다.	SI-7	10.4.1, 12.2.2, 12.2.3		CSC-3	§164.312 (c), §164.308 (a)(5)(ii)(B)	
	PR.IP-1: 기본 정보 기술/산업 규제 시스템의 기본적인 구성은 생성되고 유지한다.	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	12.4.1, 10.1.4, 10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.5.1, 12.5.2,12.5.3, 10.1.2, 10.3.2, 12.4.1, 12.5.2, 12.5.3, 10.1.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.3, 6.1.3. 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.3.2,12.4.1, 12.4.3, 12.5.1, 12.5.2, 12.5.3		CSC-2, CSC-3, CSC-4, CSC-7, CSC-13	§164.312 (c)	
	PR.PT-2: 이동식 미디어는 보호되며 사용제안은 정책에 따라 설립한다.	SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	6.1.3, 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.1.4, 10.3.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.1, 12.5.2, 12.5.3		CSC-3, CSC-7	§164.312 (c)	
	DE.CM-5: 승인되지 않은 모바일 코드는 감지한다.	SC-18, SI-4. SC-44	10.4.2, 9.10.2, 13.1.1, 13.1.2		CSC-5, CSC-6, CSC-12, CSC-14	§164.312 (c)	

	DE.CM-6: 외부 서비스 제공자 활동은 잠재적인 사이버보안 사건을 감지하기 위해 모니터링 한다.	CA-7, PS-7, SA-4, SA-9, SI-4	6.1.5, 6.1.8, 6.2.1, 6.2.3, 8.1.1, 8.1.3, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 9.10.2, 12.1.1, 12.5.5, 13.1.1, 13.1.2, 15.2.1, 15.2.2		CSC-3, CSC-5, CSC-6, CSC-7, CSC-14, CSC-15, CSC-17	§164.312 (c)	
	DE.CM-7: 허가되지 않은 사용자, 연결, 기기 및 소프트웨어에 대한 모니터링을 수행한다.	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	6.1.8, 7.1.1, 7.1.2, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 9.1.1, 9.1.2, 9.10.1, 9.10.2, 9.10.4, 9.10.5, 10.3.2, 11.4.4, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2		CSC-1, CSC-2, CSC-3, CSC-4, CSC-5, CSC-6, CSC-14, CSC-17	§164.312 (c), §164.308 (a)(5)(ii)(B)	
사용자 및 기기 인증	PR.AC-1: 신원 및 권한은 허가받은 기기와 사용자를 위해 관리한다.	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3		CSC-5, CSC-9, CSC-11	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)	
	PR.AC-3: 원격 접근은 관리한다.	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.2.2, 9.2.3, 10.6.1, 11.2.1, 11.2.2, 11.2.4, 11.3.2, 11.4.4			§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)	
	PR.AC-4: 접근 허가는 최소한의 혜택 및 분리된 책임에 관한 원칙이 적용되어 관리한다.	AC-2, AC-3, AC-5, AC-6, AC-16	6.1.3, 7.2.2, 8.1.1, 8.3.3, 10.1.3, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.2.4,		CSC-8, CSC-9	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)	

			11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2, 12.4.3, 15.2.1				
전송 보안	PR.AC-3: 원격 접근은 관리한다.	AC-17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2		CSC-5, CSC-6, CSC-8, CSC-14	§164.312 (e)	
	PR.AC-5: 네트워크 무결성은 네트워크의 적절한 분리에 의해 보호한다.	AC-4, SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 11.4.5, 11.4.6, 11.4.7, 11.7.2, 12.4.2, 12.5.4		CSC-4, CSC-5, CSC-9, CSC-13, CSC-15, CSC-16	§164.312 (e)	
	PR.DS-2: 데이터는 보호한다.	SC-8	10.4.2, 10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.2.3, 12.3.1			§164.312 (e)	
	PR.PT-4: 통신 및 규제 네트워크는 보호한다.	AC-4, AC-17, AC-18, CP-8, SC-7	9.1.4, 10.4.2, 10.6.1, 10.6.2, 10.8.1, 10.9.1, 10.9.2, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.7.1, 11.7.2, 12.2.3, 12.3.1, 12.4.2, 12.5.4, 14.1.3			§164.312 (e)	

부 록 Ⅰ-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

해당사항 없음

부 록 Ⅰ-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

해당사항 없음

부 록 Ⅰ-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

해당사항 없음

부 록 Ⅰ-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

[1] NIST 사이버 보안 프레임워크 - 주요 기반의 보호를 촉진하기 위한 표준, 가이드라인 및 모범 사례
[2] ISO/IEC 27002: 2013 정보 기술 - 보안 기술 - 정보 보안 규제에 관한 규약
[3] ISO/IEC 27799: 2016 정보 기술 - 보안 기술 - 의료정보 보안 규제에 관한 규약
[4] 20 Critical Security Controls 20개의 주요 보안 규제들
[5] 미국 사회보건복지부 (HHS). 건강 정보 기술 사무국(ONC)에서 발행한 보안 위험 평가(SRA) 도구의 기술 보호
[6] HIPAA(Health Insurance Portability and Accountability Act)
[7] NIST SP 800-53 rev.4, 연방 정보 시스템 및 기관을 위한 보안 및 프라이버시 규제
[8] NIST SP 800-66 ,건강 보험 양도 및 책임에 관한 법률(HIPAA)를 실행하기 위한 소개 가이드
[9] NIST SP 800-41 rev1, 방화벽과 방화벽 정책에 관한 가이드라인
[10] NIST SP 800-114, 재택 근무 및 원격 접근을 위해 사용되는 외부 기기 보안에 관한 가이드
[11] NIST SP 800-46 rev1, 기업 재택근무 및 원격 접근 보안에 관한 가이드
[12] NIST SP 800-77, IPsec VPN에 관한 가이드
[13] NIST SP 800-52, 전송 계층 보안(TLS) 실행의 선정, 구성 및 사용에 관한 가이드
[14] NIST SP 800-57 Part 2, 주요 관리를 위한 권고사항: 제 2부: 주요 관리 기관을 위한 모범 사례
[15] NIST SP 800-53 Part 3 rev1, 주요 관리를 위한 권고사항: 제 3부 - 응용 프로그램별 주요 관리 가이드
[16] NIST SP 800-32, 공적 주요 기술 및 연방 PKI 기반에 대한 소개
[17] NIST SP 800-30, 위험평가 시행을 위한 가이드
[18] NIST SP 800-39, 정보보안위험 기관, 미션 및 정보 시스템 관리
[19] NIST SP 800-37, 연방정보시스템에서의 위험관리 프레임워크 적용에 관한 가이드. 보안 관련 전 주기 접근법
[20] RFC 2138, 사용자 서비스에서의 원격 인증 전화 접속 (RADIUS)

부 록 Ⅰ-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2019.10.xx	TTAR.xx-xx.xxxx	디지털병원 정보보호 지침 중 사이버보안 행동강령	바이오인식 프로젝트그룹 (PG505)