

등록번호
안내서-0995-05



의료기기의 사이버보안 허가 · 심사 가이드라인(민원인 안내서)

2025. 1. 10.



식품의약품안전처

식품의약품안전평가원

의 료 기 기 심 사 부

지침서 · 안내서 제 · 개정 점검표

명칭

의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서)

아래에 해당하는 사항에 체크하여 주시기 바랍니다.

등록대상 여부	☐ 이미 등록된 지침서 · 안내서 중 동일 · 유사한 내용의 지침서 · 안내서가 있습니까?	☐ 예 ☒ 아니오
	☞ 상기 질문에 '예'라고 답하신 경우 기존의 지침서 · 안내서의 개정을 우선적으로 고려하시기 바랍니다. 그럼에도 불구하고 동 지침서 · 안내서의 제정이 필요한 경우 그 사유를 아래에 기재해 주시기 바랍니다. (사유 :)	
	☐ 법령(법 · 시행령 · 시행규칙) 또는 행정규칙(고시 · 훈령 · 예규)의 내용을 단순 편집 또는 나열한 것입니까?	☐ 예 ☒ 아니오
	☐ 단순한 사실을 대외적으로 알리는 공고의 내용입니까?	☐ 예 ☒ 아니오
	☐ 1년 이내 한시적 적용 또는 일회성 지시 · 명령에 해당하는 내용입니까?	☐ 예 ☒ 아니오
	☐ 외국 규정을 번역하거나 설명하는 내용입니까?	☐ 예 ☒ 아니오
	☐ 신규 직원 교육을 위해 법령 또는 행정규칙을 알기 쉽게 정리한 자료입니까?	☐ 예 ☒ 아니오
☞ 상기 사항 중 어느 하나라도 '예'에 해당되는 경우에 지침서 · 안내서 등록 대상이 아닙니다. 지침서 · 안내서 제 · 개정 절차를 적용하실 필요는 없습니다.		
지침서·안내서 구분	☐ 내부적으로 행정사무의 통일을 기하기 위하여 반복적으로 행정사무의 세부기준이나 절차를 제시하는 것입니까? (공무원용)	☐ 예(☞지침서) ☒ 아니오
	☐ 대내외적으로 법령 또는 고시 · 훈령 · 예규 등을 알기 쉽게 풀어서 설명하거나 특정한 사안에 대하여 식품의약품안전처의 입장을 기술하는 것입니까? (민원인용)	☒ 예(☞안내서) ☐ 아니오
기타 확인 사항	☐ 상위 법령을 일탈하여 새로운 규제를 신설 · 강화하거나 민원인을 구속하는 내용이 있습니까?	☐ 예 ☒ 아니오
	☞ 상기 질문에 '예'라고 답하신 경우 상위법령 일탈 내용을 삭제하시고 지침서 · 안내서 제 · 개정 절차를 진행하시기 바랍니다.	
상기 사항에 대하여 확인하였음.		
2025년 1월 10일 담당자 확 인(부서장)		
김 미 선 강 영 규		

개정 이력서

의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서)

제 · 개정 번호	승인일자	주요 내용
안내서-0995-01	2019.11.28.	의료기기의 사이버보안 허가심사 가이드라인(민원인 안내서) 제정
안내서-0995-02	2022.01.21.	IMDRF ‘의료기기 사이버보안 원칙 및 기준’의 적용범위, 정의, 시판 전 고려사항을 적용
안내서-0995-03	2023.07.13.	사이버보안 제출자료 요건 명시 및 변경 시 제출자료, 허가신청서 기재방법 명확화
안내서-0995-04	2024.11.27.	법 제정에 따른 적용범위 명확화, 국제규격(IEC 62443-4-2, IEC TR 60601-4-5)에 따른 요구사항 적용
안내서-0995-05	2025.01.10.	요구사항 시행시기 명확화

이 안내서는 사이버보안 허가·심사 시의 적용범위 및 판단기준 등에 대해 알기 쉽게 설명하거나 식품의약품안전처의 입장을 기술한 것입니다.

본 안내서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술 방식('~하여야 한다' 등)에도 불구하고 참고로만 활용하시기 바랍니다. 또한, 본 안내서는 '25년 1월 현재의 과학적·기술적 사실 및 유효한 법규를 토대로 작성되었으므로 이후 최신 개정 법규 내용 및 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

※ “민원인 안내서”란 민원인들의 이해를 돕기 위하여 법령 또는 행정규칙을 알기 쉽게 설명하거나 특정 민원업무에 대한 행정기관의 대외적인 입장을 기술하는 것(식품의약품안전처 지침서등의 관리에 관한 규정 제2조)

※ 본 안내서에 대한 의견이나 문의사항이 있을 경우 의료기기심사부 디지털헬스 규제지원과에 문의하시기 바랍니다.

전화번호: 043-719-3948, 3988

팩스번호: 043-719-3940



목 차



I . 일반사항

- 1. 배경 및 목적 1
- 2. 적용 범위 2
- 3. 용어의 정의 3

II . 의료기기 사이버보안 기본원칙 6

III . 의료기기 사이버보안 요구사항 9

IV . 허가·심사 첨부자료

- 1. 제출 자료의 범위 및 요건 53
- 2. 의료기기 사이버보안 요구사항 체크리스트 57
- 3. 허가·인증 변경 시 제출자료 60

V . 참고문헌 62

[별첨] 가이드라인 개정 전·후 사이버보안 요구사항 비교 .. 63

1. 배경 및 목적

정보통신기술의 발달로 유·무선 통신하는 의료기기의 개발이 증가하고 있다.

이러한 의료기기는 원격진료 목적으로 사용되는 ‘유헬스케어 의료기기’에서부터 생명 유지 기능 목적의 ‘이식형심장박동기’에 이르기까지 매우 다양하며, 기술의 발전으로 통신 가능한 다양한 유형의 의료기기가 개발될 것으로 예상된다.

그러나 의료기기의 해킹, 정보 유출 등 사이버보안 위협사례가 꾸준히 보고되고 있고, 이러한 위협사례는 재산적 손실뿐만 아니라 환자 생명에 직접적인 위협을 줄 수 있어 의료기기의 사이버보안에 대한 중요성이 부각되고 있다.

이에 본 가이드라인에서는 의료기기 허가·심사 시 사이버보안이 요구되는 의료기기의 적용 대상을 명확히 하고 제품의 특성에 따라 적용할 수 있는 보안 요구사항과 허가·심사 시 제출해야 하는 자료의 범위를 정하여 통신이 가능한 의료기기의 안전관리를 확보하고자 한다.

2. 적용 범위

본 가이드라인은 「의료기기법」에 따른 의료기기, 「체외진단의료기기법」에 따른 체외진단의료기기, 「디지털의료제품법」에 따른 디지털 의료기기 및 디지털의료기기가 조합된 디지털융합의약품에 적용한다. 본 가이드라인에서는 이를 모두 통칭하여 ‘의료기기’로 표기하며, 구체적인 대상은 다음과 같다.

유·무선 통신(Wi-Fi, 블루투스, USB, RS-232, LAN 등) 경로가 있는 의료기기로,

- 1) 펌웨어(Firmware) 또는 프로그램 가능 논리 제어기(PLC, Programmable Logic Controller) 등 소프트웨어를 포함하는 의료기기
- 2) 소프트웨어로만 존재하는 의료기기(Software as a Medical Device, SaMD)

본 가이드라인은 사이버보안 위협에 대비하여 의료기기 허가·심사 시 적용되는 최소한의 요구사항과 제출자료의 범위를 설명한 것으로, 의료기기 허가·심사 시 제출하는 ‘사이버보안 검증 자료’ 또는 ‘전자적 침해행위로부터의 보호 조치에 관한 자료’에 반영할 수 있다. 이외 개인 정보 유출 등 건강에 직접적으로 영향을 미치지 않는 사항은 의료법 및 개인정보보호법 등 타 법령을 함께 준수하도록 권장한다.

3. 용어의 정의

가. 가용성(Availability)

의료기기 정보와 기능을 원하는 시점에 안정적으로 사용할 수 있음을 보장하는 속성(IEC TR 60601-4-5:2021)

나. 기밀성(Confidentiality)

허가되지 않은 개인, 프로세스 또는 장치에 정보가 노출되지 않음을 보증하는 것(KS X IEC 62443-4-2:2019)

다. 대책(Countermeasure)

공격을 일으킬 수 있는 위해성을 최소화함으로써 위협, 취약성 또는 공격의 결과를 감소시키는 활동, 장치, 절차, 기법 또는 시정조치가 취해질 수 있도록 발견하고 보고함으로써 공격 결과를 감소시키는 방법(KS X IEC 62443-4-2:2019)

라. 무결성(Integrity)

자산의 정확성과 완전성을 보호하는 속성(KS X IEC 62443-4-2:2019)

마. 보건의료정보

보건의료와 관련한 지식 또는 부호 · 숫자 · 문자 · 음성 · 음향 · 영상 등으로 표현된 모든 종류의 자료(보건의료기본법 제3조(정의))

바. 보안(Security), 사이버보안(Cybersecurity)

정보 및 시스템이 인증, 사용 통제, 무결성, 데이터 기밀성, 데이터 흐름, 적시 대응, 가용성과 관련된 위험이 생명주기 내내 허용 가능한 수준으로 유지되는 정도로 접근, 사용, 공개, 방해, 수정, 또는 파괴와 같은 인가되지 않은 활동으로부터 보호되는 상태(IEC TR 60601-4-5:2021)

사. 소프트웨어 의료기기(Software as a Medical Device, SaMD)

하드웨어에 종속되지 않고 의료기기의 사용목적에 부합하는 기능을 가지며 독립적인 형태의 소프트웨어만으로 이루어진 의료기기

아. 암호화(Encryption)

정보보안을 유지하기 위하여 그 정보를 특정한 규칙에 따라 변형하여 저장함으로써 해독방법을 모르면 그 정보의 내용을 알아볼 수 없도록 하는 기술

자. 인증(Authentication)

요청된 개체의 신원 검증(KS X IEC 62443-4-2:2019)

차. 자산(Asset)

의료기기 또는 의료용 IT네트워크에 대해 인지되거나 실제 가치가 있는 물리적 또는 논리적 객체(IEC TR 60601-4-5:2021)

카. 진본성(Authenticity)

개체가 원본의 인증 및 무결성 검증을 통해 소유하고 있다고 주장하는 속성(KS X IEC 62443-4-2:2019)

타. 최소권한(Least Privilege)

사용자(사람, 소프트웨어 프로세스 또는 기기)에게 부여된 임무와 기능에 적합한 최소의 권한을 부여해야 한다는 원칙(KS X IEC 62443-4-2:2019)

파. 필수 기능(Essential Function)

의료기기에 대한 기본(Basic) 안전, 필수 성능, 제조자가 명시한 최소한의 임상적 기능성, 그리고 운영 가용성을 유지하기 위해 요구되는 기능 또는 역량(IEC TR 60601-4-5:2021)

※ 의료기기 위험관리 관련 용어는 「의료기기 제조 및 품질관리 기준 (식약처 고시)」 및 ISO 14971:2019¹⁾를 참조한다.

※ 기타 사이버보안 관련 용어는 IEC 62443-4-2:2019²⁾, KS X IEC 62443-4-2:2019³⁾, IEC TR 60601-4-5:2021⁴⁾을 참조한다.

1) Medical devices - Application of risk management to medical devices

2) IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components

3) KS X IEC 62443-4-2:2019, 산업제어시스템 보안 - 제4-2부: 산업제어시스템 컴포넌트의 기술적 보안 요구사항

4) IEC TR 60601-4-5:2021, Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications

II

의료기기 사이버보안 기본원칙

의료기기 사이버보안은 가용성(Availability), 기밀성(Confidentiality), 무결성(Integrity)을 고려하여야 한다.

가용성은 데이터가 승인된 사용자에게 즉시 제공되어야 하며, 필요한 때에 필요한 곳에서 필요한 형태로 존재되어야 함을 의미한다.

기밀성은 데이터가 허가되지 않은 사람에게 공개되거나, 허가되지 않은 용도로 사용되지 않아야 함을 의미한다. 제조자는 데이터의 송·수신 과정 또는 비인가자의 조회 등 비합법적인 방법이나 오류에 의해 데이터가 노출되더라도 해독하기 어렵도록 암호화하고 인가된 자에 한해 정보의 접근이 가능하도록 하며, 정보이용자도 목적과 그 권한에 따라 접근범위를 제한하여야 한다.

무결성은 데이터가 허가되지 않은 방법으로 변환되거나 파괴되지 않아야 함을 나타낸다. 정보는 정확하고 완전해야 하며, 위·변조를 통해 왜곡되지 않도록 해야 한다. 정보 변경 시 인가된 사용자에게 의해서만 이루어지고, 로그 및 변경 이력이 관리되어야 한다.

의료기기의 사이버보안 위협을 최소화하기 위하여 가용성, 기밀성, 무결성이 준수되어야 하며, 의료기기 위협관리와 같이 「의료기기 제조 및 품질관리 기준」에 따라 의료기기 제조자가 품질시스템에서 수립한 위협관리 프로세스 내에서 적용되어야 한다.

의료기기 사이버보안의 위협관리 프로세스는 위험분석(Risk analysis), 위험평가(Risk evaluation), 위험통제(Risk control), 잔여위험 허용평가(Evaluation of overall residual risk acceptability), 위협관리보고서

(Risk management report), 생산 및 생산 후 정보(Production and post-production information)의 단계로 진행된다. 이러한 사이버보안 위험 관리는 정보의 생명주기 전체에 걸쳐 통신 경로가 있는 의료기기에 적용한다.



[그림 1. 의료기기 사이버보안 위험관리 프로세스]

의료기기 사이버보안 위험분석 단계에서는 가용성, 기밀성, 무결성이 파괴되어 환자에게 미치는 위해요인을 식별한다. 또한 이러한 과정에서 식별된 위해요인이 현실화된 결과의 잠재적 영향을 평가하고, 실제적인 발생 가능성을 평가하여 위험 수준을 결정한다.

의료기기 사이버보안 위험평가 단계에서는 식별된 각 위해요인에 대하여 위험관리 계획서에 정의된 위험 수용기준을 바탕으로 산정된 위험이 위험감소를 하지 않아도 될 만큼 낮은지를 결정하여야 한다.

의료기기 사이버보안 위험통제 단계에서는 위험평가 결과를 감안한 적절한 사이버보안 위험통제 방안을 선택하고, 선택한 방안의 구현에 필요한 모든 통제를 결정 및 실행하여야 한다.

그리고 위험통제 수단을 적용한 후 잔여위험들에 대하여 허용 평가를 하여야 한다.

제조자는 이러한 일련의 사이버보안 위험관리 프로세스에서의 절차들을 위험관리보고서에 기록하여야 한다.

생산 및 생산 후 정보 단계에서는 사이버보안에 대한 정보를 검토하기 위한 체계적인 절차를 수립하고 유지하여야 한다.

또한, 제조자는 사이버보안 위험관리 프로세스를 적용하기 위해 적절한 기능과 수준으로 사이버보안 목표를 수립하여야 한다. 사이버보안 목표는 사이버보안 정책과의 일관성을 유지하고, 실현 가능한 수준에서 측정이 가능하며 적용 가능한 사이버보안 요구사항과 위험평가 및 위험처리 결과를 감안하여야 한다.

아울러, 의료기기 생명주기 전체에 걸쳐 내부 및 외부 고객들의 의견을 지속적으로 수집·분석하여 의료기기 사이버보안 위험관리에 반영한다.

의료기기 사이버보안 위험관리보고서의 구체적인 작성방법은 「의료기기의 사이버보안 적용방법 및 사례집(2022)」을 참조할 수 있다.

III

의료기기 사이버보안 요구사항

유·무선 통신 경로가 있는 의료기기는 정보의 위변조, 오작동 또는 의료 기기에 승인되지 않은 접근 등을 방지하기 위한 대책을 마련하여야 한다.

제조자는 표 1을 참고하여 의료기기의 잠재적 결함으로 인해 사용자에게 발생할 수 있는 위해의 정도, 의료기기의 통신방법 및 사용 환경을 종합적으로 고려하여 표 1의 요구사항 적용 여부를 식별하고, 식별된 요구사항에 대해 사이버보안 안전을 확인할 수 있는 검증자료를 제출하여야 한다.

[표 1. 의료기기 사이버보안 요구사항 적용을 위한 고려사항의 예]

고려 사항	종류	설명
사이버 보안 침해로 인한 위해도	상 (major)	의료기기 사이버보안 침해로 사용자의 심각한 상해 또는 사망, 신체 기능의 영구적 장애, 신체구조의 영구적 손상의 가능성이 있음
	중 (moderate)	의료기기 사이버보안 침해로 사용자의 일시적이고 경미한 상해, 의학적 중재가 필요할 수 있음
	하 (minor)	의료기기 사이버보안 침해로 사용자의 일시적인 불편, 의학적 중재 없이 가역적이거나 경미하고 단시간의 불편이 있을 수 있음
통신 방법	유선 통신	유선 케이블(USB, RS-232, HDMI 등)을 이용하여 다른 기기 및 시스템과의 통신을 수행
	무선 통신	무선 통신 모듈(Wi-Fi, 블루투스, NFC, RF 통신 등)을 이용하여 다른 기기 및 시스템과의 통신을 수행
사용 환경	병원 내 사용	병원 내에서만 사용되는 의료기기로 사이버보안 침해를 위한 제3자의 접근이 어렵고, 보안이 갖춰진 병원 폐쇄망 내에서 사용됨
	병원 외 사용	병원 외에서 사용이 가능한 의료기기(개인용 의료기기 등)로 제3자의 접근이 용이함
	공용 네트워크망 사용	시공간의 제약없이 언제, 어디서나 공용 네트워크망(인터넷 등)에 접속하여 기기 및 시스템과의 통신이 가능함

아래 표 2의 요구사항은 사이버보안 규제의 국제조화를 위해 IEC 62443-4-2:2019, KS X IEC 62443-4-2:2019 및 IEC TR 60601-4-5:2021 규격의 요구사항을 적용한 것으로 현지점에서 사용되고 있는 제품들의 기술적 특성을 반영하였다. 제시된 요구사항은 의료기기 허가·심사 시 제출되어야 하는 최소한의 요구사항으로 모두 만족해야 하며, 제품의 특성 상 적용할 수 없는 일부 요구사항에 대해서는 해당 항목의 미적용 사유를 확인할 수 있는 근거자료(위험관리문서, 사용자 설명서, 설계 문서 등)를 제출하여야 한다.

추후 새로운 제품이 개발되거나 기능, 통신 특성 등이 차이가 있는 경우 사이버보안 요구사항 일부가 제외되거나 추가될 수 있다. 이러한 요구사항은 제품의 허가 이후에도 지속적인 사후관리를 통해 제품에 반영하여야 한다.

또한, 「디지털의료제품법」 제14조에 따른 「디지털의료기기 전자적 침해행위 보안지침(식약처 고시)」에서 언급하는 ‘인공지능 보안’은 사이버보안 요구사항을 추가 제시하거나, 동 가이드라인의 세부 요구사항 중 적절한 요구사항을 선별하여 추가 검증한다.

[표 2. 의료기기 사이버보안 요구사항]

항목	요구사항 번호	요구사항
식별 및 인증(IA)	IA-01	사용자 식별 및 인증
	IA-02	계정 관리
	IA-03	식별정보 관리
	IA-04	인증정보 관리
	IA-05	비밀번호 강도 설정
	IA-06	인증정보에 대한 피드백
	IA-07	연속적인 로그인 시도 실패 시 로그인 제한

항목	요구사항 번호	요구사항
	IA-08	시스템 사용 알림 메시지
사용 통제(UC)	UC-01	권한 부여
	UC-02	모바일 코드 사용 통제
	UC-03	세션 잠금
	UC-04	감사기록 생성
	UC-05	감사 처리 실패 대응
	UC-06	타임스탬프
	UC-07	부인 방지
시스템 무결성(SI)	SI-01	통신에 대한 무결성 보장
	SI-02	악성코드로부터 보호
	SI-03	보안 기능 검증
	SI-04	소프트웨어 및 정보에 대한 무결성 점검
	SI-05	입력값 검증
	SI-06	오류 시 사전 결정된 상태로 출력
	SI-07	오류 처리
	SI-08	업데이트
	SI-09	업데이트에 대한 진본성 및 무결성 검증
	SI-10	물리적 변조 방지
	SI-11	부트 프로세스 무결성 검증
데이터 기밀성(DC)	DC-01	정보에 대한 기밀성 보장
	DC-02	보건의료정보 비식별화
	DC-03	안전한 암호화 사용
이벤트 적시 대응(TRE)	TRE-01	감사로그에 대한 비인가된 접근 제한
자원 가용성(RA)	RA-01	서비스 거부(Denial of Service, DoS) 방지
	RA-02	의료기기 백업
	RA-03	의료기기 복구 및 재구성
	RA-04	네트워크 및 보안 구성 설정
	RA-05	불필요한 기능 비활성화

각 요구사항을 기반으로 시험을 수행하고, 결과를 판정할 때 다음 사항을 고려한다.

1) 각 요구사항 기반으로 시험을 하거나 참조하여 의료기기 사이버 보안 기능을 구현하는 경우, 해당 사이버보안 요구사항은 의료기기의 기본 안전과 필수 성능에 부정적인 영향을 주지 않아야 한다.

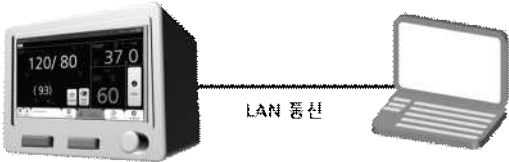
2) 의료기기는 자체적으로 사이버보안 요구사항에 대응되는 보안 기능을 제공하지 못할 수도 있지만 상위 개체(예. 병원 IT네트워크 또는 부서 IT네트워크)에서 제공하는 기능의 도움을 받을 수 있도록 설계할 수 있다. 의료기기 사용 환경 및 상황에 따라 보안 기능 구현방법은 달리 적용될 수 있으며, 제품의 특성상 상위 개체의 보안 기능을 이용하는 경우 이에 대한 보안 기능 구현의 적절성과 타당성을 제시하여야 한다.

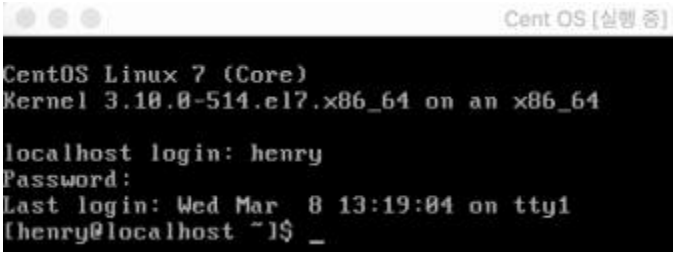
3) 악의적인 목적을 가진 사용자(예. 공격자)에 의한 공격은 의료용 IT네트워크가 지원하는 기능과 의료기기 자체의 일부 기능의 손실로 이어질 수 있다. 이러한 경우 의료기기는 필수 기능을 유지할 수 있어야 한다.

다음은 표 2의 요구사항에 따른 세부 요구사항과 세부 요구사항에 대한 최소한의 시험기준, 시험방법, 적용 예외사항을 설명한 것이다. 요구사항별 시험기준과 시험방법은 대표적인 예시를 들어 작성한 것으로 의료기기에 구현된 요구사항에 따라 차이가 있을 수 있다.

식별 및 인증(IA, Identification and Authentication)

□ IA-01 사용자 식별 및 인증

구분	내용
세부 요구사항	- 사용자(사람, 소프트웨어, 기기)가 접근할 수 있는 모든 인터페이스마다 사용자를 식별하고 인증할 수 있는 기능이 있어야 한다. 이 기능은 상위 시스템의 식별 및 인증 시스템에서 제공하거나 의료기기에 자체적으로 구현할 수도 있다. * 접근할 수 있는 인터페이스 예: LAN, USB, WiFi 등 * 사용자 식별 및 인증은 다중 접속 금지 기능을 포함함 - 환자의 생명에 직접적인 영향을 미치는 의료기기와 통신하는 제품* 및 소프트웨어 의료기기(SaMD)의 경우 의료기기 자체적으로 사용자의 식별 및 인증 기능을 구현하는 것을 우선 고려하여야 한다. * 예. 체외용인슐린주입기 등 약물을 주입하는 의료기기와 통신하는 모바일 의료용 앱, 이식형심장박동기·이식형심장충격기 등과 통신하는 심장박동기 분석기 및 모바일 의료용 앱 등
시험기준	다음 중 하나 이상 만족해야 하며, 식별 및 인증 기능이 정상 동작하여야 한다. - 의료기기는 접근 가능한 각 인터페이스별로 사용자 식별 및 인증 기능을 구현한다. - 의료기기는 상위 시스템에서 제공하는 인증 기능을 이용할 수 있다. 예) 아이디·비밀번호 기반 인증, 사전 공유키 또는 USB 토큰, 공유 계정
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 사용자를 확인한다. 2) 식별된 사용자가 접근 가능한 모든 인터페이스를 확인한다. - 시험대상예 LAN 연결 후 SSH 통신 도구를 이용하여 접근을 시도하고, 연결 시 아이디/비밀번호를 요청하는 것을 확인한다. 접근 대상에 OS 등이 설치되어 있을 경우 루트(Root) 계정 접근제어 기능이 존재하는지 확인한다. * 문서에 식별되지 않은 사용자가 접근 가능한지 인터페이스 점검  LAN 통신 <시험 환경>  <SSH 접근>

	3) 식별된 인터페이스에 접근하여 접근제어 동작 여부를 확인한다.  <비밀번호 입력 확인 예) QWer*1234> (예시) - 시험환경 구축 후 의료기기에 접속 가능한 외부 인터페이스(예. 웹브라우저 등)를 실행하여 의료기기에 접속을 시도(예. 시험대상 URL 및 포트 정보 입력) - 접속 시도 후, 아이디와 비밀번호로 식별 및 인증 수행 여부 확인
적용 예외사항	의료기기에 사용자가 접근 가능한 인터페이스가 없는 경우에는 적용하지 않는다.

□ IA-02 계정 관리

구분	내용
세부 요구사항	- 의료기기는 모든 계정을 관리할 수 있는 기능이 있거나, 계정을 관리하는 상위 시스템의 기능을 이용할 수 있어야 한다. - 인가된 사용자에게 의해 모든 계정을 관리하는 기능(계정 추가, 활성화, 수정, 비활성화 및 삭제 등)이 있어야 한다.
시험기준	다음 중 하나 이상 만족해야 하며, 계정 관리 기능이 정상 동작하여야 한다. - 계정 관리 기능이 있다. - 상위 수준의 계정 관리 시스템을 이용할 수 있는 기능이 있다. * 상위 수준 계정 관리의 예: LDAP(Lightweight Directory Access Protocol), Active Directory 또는 호스트(예. 운영자 워크스테이션)에 연결된 의료기기 * 필수 기능 - 의료기기는 상위 시스템에 가용성 문제가 발생한 경우에도 영향을 받지 않아야 한다. - 필수 기능에 사용되는 계정은 일시적으로라도 잠기지 않아야 한다.
시험방법 (예시)	1) 의료기기에 접속하여 계정 관리 인터페이스가 있는지 확인하거나, 의료기기의 계정 관리 기능이 LDAP 등과 같은 인증 시스템의 기능을 이용하는지 확인한다. 2) 사용자(사람) 계정을 추가, 활성화, 수정, 비활성화, 삭제 기능을 시험하여 정상 동작하는지 확인한다.
적용 예외사항	의료기기에 고정된 관리자 계정이 하나만 구현되어 다른 계정을 추가할 수 없는 경우에는 적용하지 않는다.

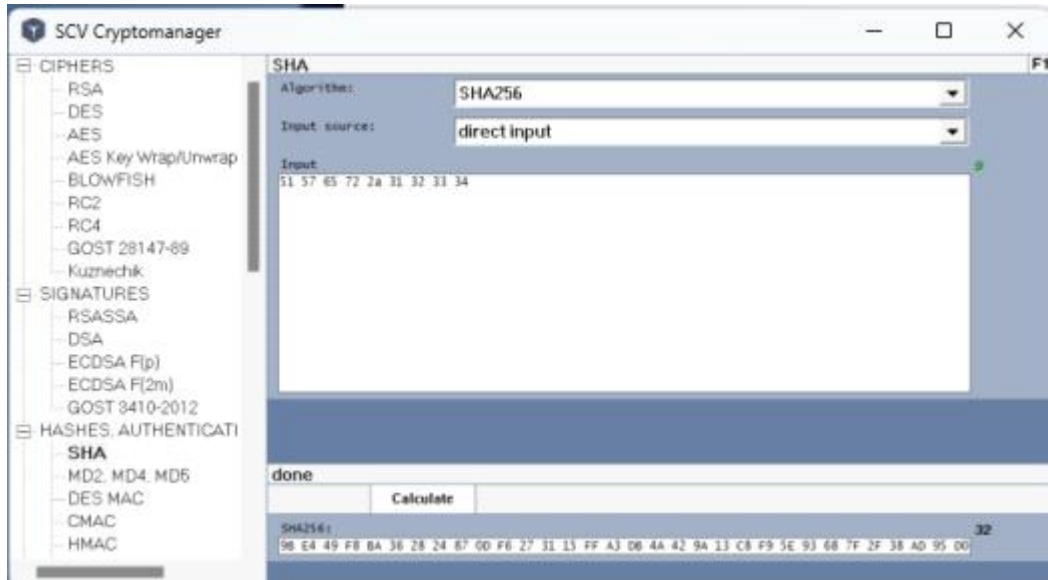
□ IA-03 식별정보 관리

구분	내용
세부 요구사항	- 의료기기는 식별정보 관리 기능이 있는 시스템을 이용할 수 있거나, 직접적으로 식별정보를 관리할 수 있는 기능이 있어야 한다. - 계정 관리(IA-02)에 의해 생성된 계정은 각 계정을 명확하게 식별하기 위해 하나 이상의 유일한 식별정보를 사용한다. 예) 식별정보 예: 계정 이름, 유닉스 사용자 ID, MS윈도우 계정 GUID(Globally unique identifiers), X.509 인증서 등
시험기준	다음 중 하나 이상 만족해야 하며, 식별정보 관리 기능이 정상 동작하여야 한다. - 식별정보 관리기능이 있는 시스템을 이용하여 식별정보를 유일하고 모호하지 않게 관리한다. - 사용자, 그룹, 역할 또는 의료기기 인터페이스별로 식별정보를 유일하고 모호하지 않게 관리하는 기능이 있다. * 필수 기능 - 필수 기능에 사용되는 계정은 일시적으로라도 잠기지 않아야 한다.
시험방법 (예시)	1) 유닉스, MS윈도우, X.509와 같은 시스템의 식별정보 관리 기능을 이용하는지 확인하거나, 식별정보를 유일하고 모호하지 않게 관리하는 기능이 있는지 확인한다. 2) 확인된 식별정보 관리 기능이 정상적으로 동작하는지 확인한다.

□ IA-04 인증정보 관리

구분	내용
세부 요구사항	- 초기 인증정보 방식을 사용할 수 있어야 한다. 예) 토큰, 대칭키, 개인키(공개키/개인키 쌍의 부분), 생체 인식, 암호, 물리적 키 및 키 카드, 비밀번호 등 - 설치 후 디폴트 인증정보를 강제로 변경하거나, 디폴트 인증정보가 변경되지 않았을 경우 이를 알 수 있도록 기능이 있어야 한다. - 주기적으로 인증정보를 변경할 수 있는 기능이 있어야 한다. - 인증정보는 저장, 사용 및 전송 중에 공개되거나 변경되지 않아야 한다. * 비밀번호 기반 의료기기인 경우 예시 - 관리자는 모든 신규 계정에 초기 비밀번호를 설정한다. 초기 비밀번호 설정은 공격자가 계정 생성과 처음 계정 사용(계정 소유자에 의한 신규 비밀번호 설정을 포함) 사이에 비밀번호 추측을 더 어렵게 만든다. - 설치 후 디폴트 비밀번호를 변경하도록 한다. - 주기적으로 비밀번호를 변경하거나 새로고침을 하도록 한다. 이때, 변경 주기를 명시해야 한다. - 비밀번호 전송을 요구하지 않는 핸드셰이크 프로토콜 또는 암호화나 해싱 같은 암호 기반 기능을 적용한다.
시험기준	다음 사항을 모두 만족해야 하며, 인증정보 관리 기능이 정상 동작하여야 한다. - 의료기기 최초 접속 시 초기 인증정보 방식이 있다. - 설치 후 디폴트 인증정보를 강제로 변경하거나, 디폴트 인증정보가 변경되지 않았을 경우 경고 메시지 등으로 이를 알 수 있도록 한다. - 인증정보를 주기적으로 변경하도록 한다. - 인증정보를 저장, 사용, 전송할 때 인증정보가 공개되거나 변경되는 것으로 부터 보호한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 서술하고 있는 인증정보 관리 기능에 대한 인터페이스를 확인한다. 2-1) 의료기기에 최초 접속시, 초기 인증정보를 입력하게 하거나 인증정보를 입력하도록 요구하는지 확인한다. 2-2) 초기 인증정보가 존재하는 경우 초기 인증정보 입력 후 초기 인증정보를 변경하도록 하는지 확인한다. 3) 의료기기의 계정 관리 기능에 접속하여 인증정보 변경 주기를 설정하도록 하는지 확인한다. * 변경 주기가 고정되어 변경하지 못하는 경우, 변경 주기가 적합한지 확인한다.

- 4) 인증정보를 평문으로 저장, 사용, 전송하지 않는지 확인한다.
- 비밀번호의 경우, 단방향 암호화되었는지 암호화 점검 도구로 확인한다.



평문 비밀번호: QWer*1234

단방향 암호화 (SHA256) 결과: 9BE449F8BA362824870DF6273115FFA3DB4A4
29A13C8F95E93687F2F38AD95D0

<인증정보 단방향 암호화 확인>

□ IA-05 비밀번호 강도 설정

구분	내용
세부 요구사항	비밀번호 기반 인증 기능이 있는 의료기기의 경우, 비밀번호 강도를 비밀번호 설정 지침에 따라 강제로 설정하는 기능이 있거나, 설정 기능이 있는 시스템을 이용할 수 있다.
시험기준	다음 중 하나 이상 만족해야 하며, 비밀번호 강도 설정 기능이 정상 동작하여야 한다. - 비밀번호 설정 또는 변경 시 비밀번호 설정 지침(예. 정보통신망연결기기등 정보보호인증기준 상세 해설서)에 따른 비밀번호 강도를 적용한다. - 비밀번호 설정 지침을 적용한 강력한 외부 인증이 있는 시스템을 사용한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 의료기기의 비밀번호 강도가 적절한지 확인한다. 2) 1번에서 비밀번호 강도가 적절한 경우, 조합규칙에 따라 비밀번호를 설정하고 변경할 수 있는지 확인한다. 3) 조합규칙에 맞지 않는 비밀번호로 설정 또는 변경하고자 하는 경우 비밀번호를 다시 입력하게 하거나, 설정되지 않는지 확인한다.
적용 예외사항	비밀번호 기반 인증 기능이 없는 의료기기의 경우 적용하지 않는다.

□ IA-06 인증정보에 대한 피드백

구분	내용
세부 요구사항	의료기기의 인증 기능이 있는 경우 인증 과정에서 인증정보에 대한 피드백은 명확하지 않아야 한다.
시험기준	비밀번호, 무선 키, 토큰을 마스킹(예. 별표(*)) 대신 일반 텍스트로 표시하지 않으며, 인증 피드백에 인증 실패 정보가 포함되지 않아야 한다. 예) “모르는 사용자 이름(unknown user name)” 같이 인증 실패 이유에 대한 힌트
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 인증정보 피드백 보호 기능을 확인한다. 2) 로그인 등 인증정보 입력 시, 인증정보가 평문으로 보이는지 확인한다. 3) 로그인 등 과정에서 사용자(사람) 인증 실패 시, 인증 피드백에 명확한 인증 실패 정보가 포함되어 있는지 확인한다.
적용 예외사항	의료기기의 인증 기능이 없는 경우 적용하지 않는다.

□ IA-07 연속적인 로그인 시도 실패 시 로그인 제한

구분	내용
세부 요구사항	의료기기의 인증 기능이 있는 경우 다음과 같은 기능이 있어야 한다. - 설정한 시간 동안 모든 사용자(사람, 소프트웨어, 기기)가 연속적으로 잘못된 접근을 시도하는 경우 로그인 시도 횟수를 제한해야 한다. - 이러한 횟수 제한에 도달했을 때 정해진 시간 동안 또는 관리자가 잠금 해제할 때까지 접근을 거부해야 한다. 관리자는 타임아웃이 만료되기 전에 계정을 잠금 해제할 수도 있다.
시험기준	다음 사항을 모두 만족해야 하며, 로그인 제한 기능이 정상 동작하여야 한다. - 각 사용자 유형(사람, 소프트웨어, 기기)에 대해 설정된 시간 동안 연속적인 잘못된 접근 시도가 있는 경우 설정된 로그인 제한을 강제하는 기능이 있다. - 한도에 도달하면, 지정된 기간 동안 또는 잠금이 해제될 때까지 접근을 거부하는 기능이 있다. * 필수 기능 - 필수 기능에 사용되는 계정은 일시적으로라도 잠기지 않아야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 연속적인 로그인 시도 실패 횟수 설정 기능, 설정된 로그인 시도 횟수 도달 시 로그인 제한 기능(예. 관리자가 잠금 해제하기 전까지 계정 잠금, 설정된 기간 동안 계정 잠금 등)을 확인한다. 2) 로그인 시도 횟수(예. 5회 이하)를 설정한다. 3) 2번에서 설정된 로그인 시도 횟수 도달 전까지 정상적으로 로그인을 시도할 수 있는지 확인한다. 4-1) 2번에서 설정된 로그인 시도 횟수 도달 시, 설정된 로그인 제한 기능이 정상 동작하는지 확인한다. 4-2) 설정된 시간 이후 또는 관리자에 의해 잠금 해제 전까지 로그인 되지 않으며, 잠금 해제 이후 정상적으로 로그인이 되는지 확인한다.
적용 예외사항	의료기기의 인증 기능이 없는 경우 적용하지 않는다.

□ IA-08 시스템 사용 알림 메시지

구분	내용
세부 요구사항	사용자(사람)가 의료기기의 사용자 인터페이스를 직접 조작할 수 있는 경우, 인증 과정에서 시스템 사용 알림 메시지를 보여주는 기능이 있어야 하며, 시스템 사용 알림 메시지는 인가된 직원에 의해 설정 가능해야 한다. * 시스템 사용 알림 메시지 예 시스템 사용 알림 메시지는 개인이 의료기기에 로그인할 때 보이는 경고 배너 형식으로 구현될 수 있다. 다만, 원격 로그인 시 물리적으로 부착된 경고 배너는 적용할 수 없다. 시스템 사용 알림 메시지 예는 다음과 같다. - 개인 자산 소유자가 소유한 시스템에 접근함 - 시스템 사용은 모니터링, 기록 및 감사 대상이 될 수 있음 - 인가되지 않는 시스템 사용은 금지되고 민·형사 상의 처벌대상임 - 시스템의 사용은 모니터링과 기록에 동의함을 의미함
시험기준	다음 사항을 모두 만족해야 하며, 시스템 사용 알림 메시지 기능이 정상 동작하여야 한다. - 인가된 사용자(사람)에 의해 시스템 사용 알림 메시지를 설정할 수 있는 기능이 있다. - 인증 과정 중 로컬 사용자(사람) 인터페이스를 통해 시스템 사용 알림 메시지를 표시하는 기능이 있다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 시스템 사용 알림 메시지를 설정할 수 있는 권한(역할)과 의료기기 접근 시 사용자(사람)에게 시스템 사용 알림 메시지 표시 기능을 확인한다. 2) 1번에서 확인된 권한이 있는 사용자(사람)에게만 시스템 사용 알림 메시지를 설정할 수 있는 기능이 있는지 확인한다. 3) 2번에서 설정된 시스템 사용 알림 메시지가 의료기기에 접근하는 로컬 사용자(사람)에게 표시되는지 확인한다.
적용 예외사항	시스템에 대한 접근 기능이 없는 의료기기는 적용하지 않는다.

사용 통제(UC, Use Control)

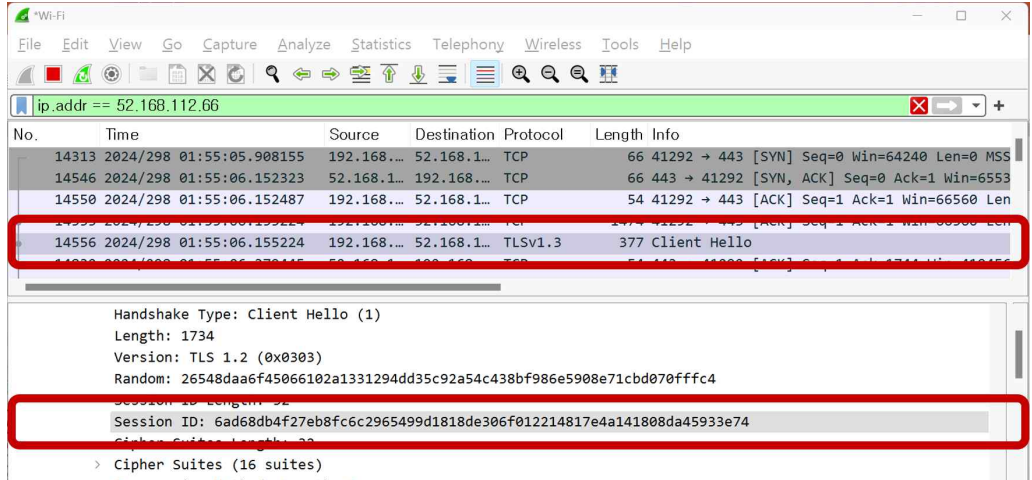
□ UC-01 권한 부여

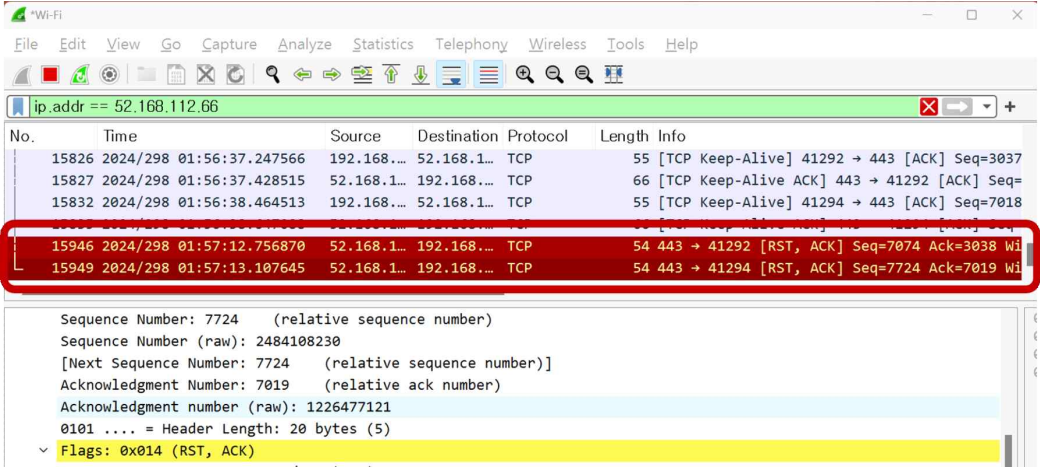
구분	내용
세부 요구사항	의료기기는 부여된 책임(responsibility)에 따라 식별 및 인증된 모든 사용자에게 권한을 부여하는 기능이 있어야 한다.
시험기준	다음 사항을 모두 만족해야 하며, 권한 부여 기능이 정상 동작하여야 한다. - 사용자(사람, 소프트웨어, 기기)의 식별 및 인증 기능이 있다. - 인증된 사용자에게 대하여 권한과 역할이 정의되어 있다. - 권한 부여 시 최소권한을 적용하고, 부여된 권한에 따라 해당 기능에만 접근 및 사용 가능한지 확인한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 사용자 역할을 확인하고 사용자 역할에 따른 권한이 최소권한 원칙에 적합한지 확인한다. 2) 의료기기의 계정 관리에 접근해서, 1번에서 확인된 사용자 역할(예. 관리자, 일반 사용자)에 따라 사용자를 추가한다. 3) 2번에서 추가된 사용자별로 의료기기에 로그인한 후, 해당하는 기능에만 접근 및 사용 가능한지 확인한다.
적용 예외사항	의료기기에 고정된 관리자 계정이 하나만 구현되어 다른 계정을 추가할 수 없는 경우에는 적용하지 않는다.

□ UC-02 모바일 코드 사용 통제

구분	내용
세부 요구사항	의료기기가 모바일 코드 기술을 활용할 경우 의료기기는 모바일 코드 기술 사용에 관하여 최소한 다음과 같은 사용 통제 기능이 있어야 한다. - 모바일 코드 실행 통제 - 사용자(사람, 소프트웨어, 기기)가 모바일 코드 송수신 허용 통제 - 모바일 코드 실행 전에 무결성 점검의 결과를 기반으로 모바일 코드 실행 통제 * 모바일 코드 - 수신자가 명시적으로 설치하지 않아도 실행되는 자산들 사이에 전송되는 프로그램 - JavaScript, VBScript, Java Applets, ActiveX 컨트롤, Flash 애니메이션, Shockwave 동영상 및 마이크로소프트 오피스 매크로 등이 있으며, 사용자의 별도 상호작용 없이 자동으로 다운로드 받은 환경에서 단독 실행되는 코드를 포함한다.
시험기준	다음 사항을 모두 만족해야 하며, 모바일 코드 사용 통제 기능이 정상 동작하여야 한다. - 모바일 코드 사용에 대한 보안 정책을 시행할 수 있는 기능이 있다. - 모바일 코드의 실행을 제어한다. - 모바일 코드를 의료기기와 송수신하도록 허용하는 사용자를 정의한다. - 의료기기에 파일을 업로드만 하고, 모바일 코드 실행을 하지 않는다. - 모바일 코드 실행 전 무결성 검사를 수행한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 모바일 코드 사용 통제 기능에 대해 정상 동작하는지 확인한다. 2) 모바일 코드를 다운로드 받아 실행 전 진위성(예. 전자서명 검증) 또는 무결성 검사 수행 후 이상 없을 때 모바일 코드를 실행하는지 확인한다.
적용 예외사항	의료기기가 모바일 코드 실행을 허용하지 않는 경우 적용하지 않는다.

□ UC-03 세션 잠금

구분	내용
세부 요구사항	로컬 또는 네트워크를 통해 의료기기에 사용자(사람)가 접속하는 경우, 의료기기는 다음과 같은 기능이 있어야 한다. - 설정 시간 동안 사용하지 않거나 사용자(사람, 소프트웨어, 기기)가 수동으로 시작하지 않으면 세션 잠금을 시작하여 추가 접근 방지 - 세션 잠금이 되면, 해당 세션을 사용하던 사용자(사람)이나 권한이 있는 다른 사용자(사람)가 적절한 로그인 절차를 통해 다시 접근하기 전까지 잠금 상태 유지
시험기준	로컬 또는 네트워크를 통한 모든 사용자 인터페이스에 대해 다음 사항 중 하나 이상을 만족해야 하며, 세션 잠금 기능이 정상 동작하여야 한다. - 설정한 비활성 시간 후 세션을 잠금 한다. - 수동으로 세션을 잠금 한다. - 인증 절차를 통해서만 세션에 접근 가능하다. - 기본 인프라(운영체제, 의료기기 시스템)에서 요청한 세션 잠금을 준수한다. * 필수 기능 - 세션 잠금 기능은 안전 기능에 부정적인 영향을 주지 않아야 한다. - 필수 기능에 사용되는 계정은 일시적으로라도 잠그지 않아야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 세션 잠금 기능을 확인한다. 2) 의료기기는 세션 잠금 시간을 확인하고 설정된 시간이 경과하는 동안 아무런 작업을 수행하지 않고 세션 잠금이 되는지 확인한다. 3) 세션 잠금 후 의료기기에 접속을 위해 재인증하는지 확인한다. - 네트워크 통신 유희 시 후 네트워크 종료되는 것을 확인하고, 재연결 시 새로운 세션 생성 여부를 네트워크 모니터링 도구(예. Wireshark)로 확인한다. 

	 Sequence Number: 7724 (relative sequence number) Sequence Number (raw): 2484108230 [Next Sequence Number: 7724 (relative sequence number)] Acknowledgment Number: 7019 (relative ack number) Acknowledgment number (raw): 1226477121 0101 = Header Length: 20 bytes (5) Flags: 0x014 (RST, ACK)
적용 예외사항	- 로컬 또는 네트워크를 통해 의료기기에 대한 접속 기능을 제공하지 않는 경우 적용하지 않는다. - 세션 종료 기능이 있는 경우 세션 잠금 기능을 만족하는 것으로 한다.

□ UC-04 감사기록 생성

구분	내용
세부 요구사항	- 의료기기는 '접근통제, 요청 오류, 의료기기 이벤트, 백업 및 복구 이벤트, 설정 변경, 감사로그 이벤트'와 같은 보안 유형과 관련된 감사기록을 생성하는 기능이 있어야 한다. - 개별 감사기록은 타임스탬프, 출처, 카테고리, 유형, 이벤트 ID, 이벤트 결과와 같은 사항을 포함해야 한다.
시험기준	다음 사항을 모두 만족해야 하며, 감사기록 생성 기능이 정상 동작하여야 한다. - 접근통제, 요청 오류, 의료기기 이벤트, 백업 및 복구 이벤트, 설정 변경, 감사로그 이벤트와 같은 보안 관련 유형에 대한 감사기록을 생성한다. - 감사기록에는 최소한 타임스탬프, 출처, 카테고리, 유형, 이벤트 ID, 이벤트 결과 등의 정보를 포함한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 감사기록 생성 대상의 감사 이벤트를 확인한다. 2) 의료기기에서 감사 이벤트 발생 시 감사기록을 정상적으로 생성하는지 확인한다.

□ UC-05 감사 처리 실패 대응

구분	내용
세부 요구사항	- 감사 처리 실패 이벤트(소프트웨어/하드웨어 오류, 감사 추출 기능의 실패 및 감사 저장 용량 초과 등) 시 필수 서비스와 기능 손실에 대비하기 위한 기능이 있어야 한다. - 감사 처리 실패에 대응하여 적절한 작업을 지원하는 기능(예. 직원에게 알람, 메시지 등과 같은 수단을 통해 경고)이 있어야 한다.
시험기준	다음 중 하나 이상을 만족해야 하며, 감사 처리 실패 대응 기능이 정상 동작하여야 한다. - 감사 처리 실패 시 필수 서비스 또는 기능의 손실이 없다. - 감사 처리 실패에 대한 적절한 조치를 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 감사 저장 용량 초과 시 대응 기능을 확인한다. 2) 감사 저장 용량이 초과하도록 감사기록을 생성하여 의료기기의 대응행동을 확인한다. 3) 2번의 경우에 의료기기의 필수 기능이 정상적으로 동작하는지 확인한다.

□ UC-06 타임스탬프

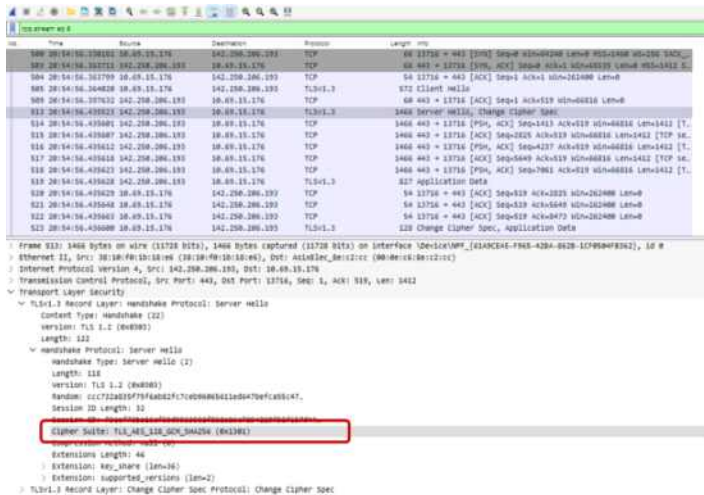
구분	내용
세부 요구사항	의료기기는 감사기록에서 사용하는 타임스탬프(날짜 및 시간 포함) 생성 기능이 있어야 한다.
시험기준	다음 사항을 모두 만족해야 하며, 타임스탬프 기능이 정상 동작하여야 한다. - 감사기록에 대한 타임스탬프 생성 기능이 있다.(UC-04 참조) - 타임스탬프에는 날짜와 시간을 포함한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 타임스탬프 생성 방법을 확인한다. 2) 의료기기 운영체제 시간 또는 NTP(Network Time Protocol) 서버를 기반으로 타임스탬프를 생성하는지 확인한다. 3) 로그인 등을 수행하여 감사기록 생성 시 타임스탬프를 정확하게 생성하는지 확인한다.

□ UC-07 부인 방지

구분	내용
세부 요구사항	의료기기에 사용자(사람) 인터페이스가 있는 경우, 해당 사용자(사람)가 특정 행동을 했는지 여부를 판단하는 기능이 있어야 한다. * 사용자의 특정 행동의 예시 사용자(사람) 작업 수행, 의료기기 설정 변경, 정보 생성, 메시지 전송, 정보 승인 (동의 표시 같은) 및 메시지 수신 등 * 부인 방지 서비스를 위한 기술 및 기능 예시 사용자 식별 및 인가, 전자서명, 디지털 메시지 수신 및 타임스탬프
시험기준	다음 사항을 모두 만족해야 하며, 부인 방지 기능이 정상 동작하여야 한다. - 사용자의 특정 행동에 대해 감사기록을 생성한다. - 감사기록에 사용자를 식별할 수 있는 정보를 포함한다. * 필수 기능 - 부인 방지는 필수 기능에 상당한 지연을 주지 않아야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 부인 방지 기능을 확인한다. 2) 의료기기가 사용자의 특정 행동에 대해 감사기록을 생성하고, 감사기록에 사용자를 식별할 수 있는 정보를 포함하는지 확인한다.
적용 예외사항	의료기기에 사용자(사람) 인터페이스가 없는 경우 적용하지 않는다.

시스템 무결성(SI, System Integrity)

□ SI-01 통신에 대한 무결성 보장

구분	내용
세부 요구사항	의료기기는 전송된 정보의 무결성을 보호하는 기능이 있어야 한다.
시험기준	다음 중 하나 이상을 만족해야 하며, 전송된 정보의 무결성 보호 기능이 정상 동작하여야 한다. - 표준화된 암호화 프로토콜을 사용한다. - 권장 프로토콜(예. KS X IEC 62443-4-2 CR 4.3에 언급된 기타 예시)을 사용한다. (DC-03 참조)
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 전송 정보의 무결성 보호 기능을 확인한다. 2) 네트워크 트래픽 모니터링 도구를 사용하여 의료기기가 정보 전송 시 암호화 프로토콜(예. TLS 1.2/1.3) 등을 사용하여 무결성을 보호하는지 확인한다. - 네트워크 모니터링 환경 구축 후 패킷을 모니터링하여 네트워크 모니터링 도구 (예. Wireshark) 등으로 통신 관련 무결성 점검 여부를 확인한다.  <패킷 모니터링 환경>  <TLS1.3 Ciphersuite 확인 결과: Cipher Suite: TLS_AES_128_GCM_SHA256>

□ SI-02 악성코드로부터 보호

구분	내용
세부 요구사항	- 소프트웨어 의료기기(SaMD)에 적용: 소프트웨어 의료기기(SaMD) 제조자는 해당 의료기기(SaMD 포함)와 호환되는 악성코드 방지 기능을 확인하고 문서화하며, 악성코드 방지를 위해 필요한 설정이나 조건이 있는 경우 이를 기록해야 한다. * 악성코드로부터의 보호는 외부 서비스, 애플리케이션에 의해 제공될 수도 있다. - SaMD 이외 의료기기에 적용: 의료기기는 인가되지 않은 소프트웨어(악성코드를 포함할 수 있음)의 설치 및 실행으로부터 보호하는 기능이 있어야 한다. * 악성코드의 예시 바이러스, 웜, 트로이 목마, 스파이웨어 등
시험기준	1) 소프트웨어 의료기기(SaMD)인 경우 사용자 설명서에 보호 기능을 구현하는 호환 가능한 보안 기능이 하나 이상 기재되어 있으며, 정의된 악성코드 대응 기능을 통해 의료기기를 보호해야 한다. 2) SaMD 이외 의료기기인 경우 다음 중 하나 이상을 만족해야 하며, 정의된 악성코드 대응 기능을 통해 의료기기를 보호해야 한다. - 승인되지 않은 소프트웨어의 설치 및 실행으로부터 보호할 수 있는 기능이 있다. - 운영환경에서 악성코드 보호 기능이 있는 경우 적용한다. - 허용된 탐지 기술을 사용한다: 바이너리 무결성, 속성 모니터링, 해싱, 서명 기술 - 허용된 방지 기술을 사용한다: 이동식 미디어 제어, 샌드박스 기술, 특정 컴퓨팅 플랫폼 기능(예. 제한된 펌웨어 업데이트), 실행 금지(NX) 비트, 데이터 실행 방지(DEP), 주소 공간 레이아웃 무작위화(ASLR)*, 스택 손상 탐지, 필수 접근 통제, 프로세스 화이트리스트 및 이와 유사한 기능 포함 * ASLR(Address space layout randomization): 실행시마다 메모리 주소를 변경시켜 악성코드에 의한 특정주소 호출 방지
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 악성코드 대응 기능을 확인한다. 2) 악성코드 또는 악성코드가 포함된 파일(예. 업데이트 파일 등)을 이용하여 의료기기에 유입 차단 또는 유입된 파일을 검증하여 대응(예. 설치가 되지 않거나 악성코드 탐지 정보를 알림 등)하는지 확인한다.

□ SI-03 보안 기능 검증

구분	내용
세부 요구사항	의료기기는 보안 기능의 의도된 작동을 검증하는 기능이 있어야 한다. * 보안 기능 검증의 예시 - 유럽 컴퓨터 백신 연구소(EICAR, European Institute for Computer Antivirus Research)에서 제공하는 테스트 파일을 의료기기 파일 시스템에서 검사하여 백신 프로그램이 이 테스트 파일을 탐지하고, 적절한 사고 대응 절차가 실행되는지 확인해야 한다. - 무단 계정으로 접근 시도를 통해 식별, 인증 및 사용 제어 방어책이 제대로 작동하는지 확인해야 한다. 일부 기능은 자동화하여 시험할 수 있다. - 침입탐지시스템(IDS, Intrusion Detection System)에 알려진 비악성 트래픽에 대한 규칙을 추가하여, 이 규칙에 따라 트래픽이 발생할 때 IDS가 이를 감지하고 적절한 모니터링 및 사고 대응 절차가 실행되는지 확인해야 한다. - 보안 정책과 절차에 따라 감사 로그가 기록되고 있으며, 내부 또는 외부 요인에 의해 비활성화되지 않았는지 확인해야 한다. * IEC 62443-3-3 SR 3.3 요구사항 의료기기는 FAT(Factory Acceptance Testing), SAT(Site Acceptance Testing) 및 예정된 유지보수 중에 이상 징후가 발견될 경우 보안 기능의 의도된 작동을 확인하는 기능을 제공해야 한다. 이러한 보안 기능은 동 표준에 명시된 보안요구사항을 지원하는데 필요한 모든 것이 포함되어야 한다.
시험기준	다음 사항을 모두 만족해야 하며, 보안 기능 검증 기능이 정상 동작하여야 한다. - 보안 기능 검증을 위한 자동 또는 수동 검증 절차를 정의하고 있다. - 의료기기의 보안 기능 검증 절차에 따라 보안 기능에 대해 검증할 수 있는지 확인한다. - 의료기기의 보안 기능 동작에 따른 결과(성공, 실패)에 대해 생성된 감사기록을 통해 보안 기능이 정상 동작여부를 알 수 있는지 확인한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 보안 기능 검증 지침/방법, 보안 기능 동작 결과(성공, 실패)에 대한 감사기록 생성 내용을 확인한다. 2-1) (검증 지침 제공 시) 보안 기능 검증 지침에 따라 의료기기의 보안 기능을 검증할 수 있는지 확인한다. 2-2) (감사기록 생성 시) 의료기기에 구현된 보안 기능을 실행한 후 감사기록을 생성하는지 확인한다.

□ SI-04 소프트웨어 및 정보에 대한 무결성 점검

구분	내용
세부 요구사항	의료기기는 소프트웨어, 정보에 대한 무결성 점검 기능(무결성 점검 수행 또는 지원, 점검 결과 기록)이 있거나, 무결성 점검을 수행 또는 지원할 수 있는 시스템 기능을 이용할 수 있어야 한다.
시험기준	다음 중 하나 이상을 만족해야 하며, 무결성 점검 기능이 정상 동작하여야 한다. - 저장 데이터(예. 보안 설정, 설정, 펌웨어 구성 및 기타 정보)에 대해 무결성 점검을 수행한다. - 무결성 검사를 수행하거나 지원할 수 있는 시스템을 이용할 수 있다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 무결성 점검 대상 파일(예. 의료기기 필수 기능에 대한 프로세스, 설정 파일 등)과 무결성 점검 방법(예. 수동, 자동, 관리자 요청 등)을 확인하고, 무결성 점검 결과에 대한 기록 방법을 확인한다. 2) 무결성 점검 대상 파일을 임의로 변경한 후 무결성 점검을 통해 무결성 오류에 대한 탐지 결과를 기록(예. 감사기록)하는지 확인한다. 3) 무결성 점검 방법(예. 암호 해시)이 적절한지 확인한다.

□ SI-05 입력값 검증

구분	내용
세부 요구사항	의료기기는 의료기기의 동작에 직접 영향을 미치는 외부 인터페이스를 통한 입력이나, 의료기기 제어 입력으로 사용된 모든 입력 데이터의 구문, 길이 및 내용을 검증해야 한다. * 입력값 검증 항목 - 정의된 필드 유형에 범위를 벗어난 값의 유효성을 검증한다. - 데이터 필드에 유효하지 않은 문자를 검증한다. - 누락되거나 불완전한 데이터 및 버퍼 오버플로를 검증한다. - SQL 삽입 공격을 검증한다. - 크로스사이트스크립트를 검증한다. - 잘못된(malformed) 패킷을 검증한다.
시험기준	의료기기의 동작에 직접적인 영향을 미치는 모든 입력의 구문 및 내용에 대한 유효성 검사를 수행하고 정상 동작하는지 확인하여야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 의료기기의 외부 인터페이스(예. API, 사용자 입력 메뉴/필드)와 해당 인터페이스에 대한 유효 입력값 및 범위를 지정하고, 유효 입력값 검증 방법을 확인한다. 2) 의료기기의 모든 외부 인터페이스(예. API, 사용자 입력 메뉴/필드 등)에 정상 입력값을 입력하여 정상 동작하는지 확인한다. 3) 2번에서 시험된 외부 인터페이스별로 유효 범위를 벗어나는 비정상 입력값을 입력하여 유효하지 않다고 에러 메시지를 출력하거나 의료기기가 오동작하지 않음을 확인한다. 4) 2번에서 시험된 외부 인터페이스별로 SQL 삽입 공격, XSS 공격에 대해 내성이 있는지 확인한다.

□ SI-06 오류 시 사전 결정된 상태로 출력

구분	내용
세부 요구사항	자동화 프로세스와 연결된 의료기기는 제조자가 정의한 정상 작업을 유지할 수 없다면 사전 결정된 상태로 출력하는 기능이 있어야 한다. * 자동화 프로세스와 연결된 의료기기 예시 - 생체신호를 실시간으로 모니터링하고 이상 징후 감지 시 알람을 출력하는 환자감시장치 - 약물을 일정한 속도로 주입하는 체외용인슐린주입기 * 사전 결정된 상태 예시 - 의료기기에 오류 발생으로 정상 동작을 할 수 없는 경우 어떻게 동작할지에 대해 미리 정해놓은 설정 상태 - 예. 체외용인슐린주입기의 사전 결정된 상태로 '인슐린 주입 중단 및 사용자 알람 발생'으로 설정한 경우, 제품 오류 발생 시 즉시 인슐린 주입을 중단하고 사용자에게 알람을 울리도록 하여 사용자가 수동으로 인슐린을 주입할 수 있게 조치함
시험기준	다음 사항을 모두 만족해야 하며, 사전 결정된 상태로 출력하는 기능이 정상 동작하여야 한다. - 사전 결정된 상태의 출력에 대해 문서화한다. - 제조자가 정의한 정상 작업 상태가 아닌 안전모드(예. 장애 시 안전(fail safe))로 실행되는 경우, 사전 결정된 상태로 동작한다. * 장애 시 안전(Fail safe, TTA정보통신용어사전) - 회선, 기기, 시스템 등이 고장이나 오동작에 대비하여 구조적으로 안전하게 설계되어 있거나 이중 안전장치를 갖추고 있어서 절대 안전하다는 것을 의미하는 말. 예를 들어 장애 시 안전 시스템(fail-safe system)이라고 하면, 그 시스템의 일부분에 장애가 발생하거나 심각한 오작동이 발생해도 프로그램이나 데이터의 분실, 파손을 야기하지 않고 동작을 계속할 수 있도록 설계된 컴퓨터 시스템을 말한다. - 조작자의 실수나 오작동 또는 고장 등에 대비한 자동 안전 장치
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 의료기기가 자동화된 프로세스에 연결되어 있는지 확인하고, 공급자가 정의한 정상 작업 상태가 아닌 경우 사전 결정된 상태로 출력 설정 기능을 확인한다. 2) 의료기기가 정상 동작이 유지되지 않는 상황에서 사전 결정된 상태로 출력하는지 확인한다.
적용 예외사항	의료기기가 자동화 프로세스와 연결되지 않는 경우 적용하지 않는다.

□ SI-07 오류 처리

구분	내용
세부 요구사항	의료기기는 의료기기 또는 의료용 IT네트워크를 공격하는 공격자에 의해 악용될 수 있는 정보를 제공하지 않는 방식으로 오류 조건을 식별하고 처리해야 한다. * 공격자에게 도움을 줄 수 있는 오류 메시지의 예시 인증의 실패 원인에 대한 상세 정보를 제공하는 것으로, 올바르지 않은 사용자 ID나 올바르지 않은 비밀번호를 제시하는 피드백은 공격자가 의료기기를 공격하는데 도움을 줄 수 있다.
시험기준	오류 조건을 식별하고 처리하며, 오류 발생 시 중요정보가 유출되지 않아야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 사용자에게 반환되는 오류 메시지 목록을 확인한다. 2) 정의된 오류 상황에 대해 의료기기가 정상적으로 오류 메시지를 출력하는지 확인한다. 3) 2번을 통해 의료기기에서 출력된 오류 메시지에 중요정보가 포함되어 있는지 확인한다.

□ SI-08 업데이트

구분	내용
세부 요구사항	의료기기는 업데이트 또는 업그레이드 기능이 있어야 한다.
시험기준	업데이트 또는 업그레이드할 수 있는 기능이 있어야 하며, 필수 기능에 영향을 주지 않고 패치 및 업데이트가 진행되어야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 업데이트 또는 업그레이드 기능을 확인한다. 2) 의료기기의 업데이트 또는 업그레이드 기능을 이용하여 업데이트 및 업그레이드가 정상적으로 수행되는지 확인한다. 3) 2번을 통해 업데이트 또는 업그레이드가 수행된 의료기기가 정상 동작하는지 확인한다.

□ SI-09 업데이트에 대한 진본성 및 무결성 검증

구분	내용
세부 요구사항	의료기기는 설치 전에 소프트웨어 업데이트 또는 업그레이드의 진본성과 무결성을 검증해야 한다.
시험기준	시험항목 SI-08와 연계하여 업데이트 또는 업그레이드 파일 설치 전에 진본성 및 무결성을 확인하고 이상이 없을 때만 설치되어야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 소프트웨어 업데이트 또는 업그레이드 파일에 대한 진본성과 무결성 검증 방법을 확인한다. 2) SI-08 시험항목과 연계하여, 업데이트 또는 업그레이드 파일 설치 전에 업데이트 또는 업그레이드 파일에 대한 진본성과 무결성을 검증하여 이상이 없을 때만 설치가 되는지 확인한다. 3) 비정상적인 업데이트 또는 업그레이드 파일(예. 잘못된 전자서명 적용)에 대해서는 업데이트 또는 업그레이드가 진행되지 않음을 확인한다.

□ SI-10 물리적 변조 방지

구분	내용
세부 요구사항	의료기기는 인가되지 않은 물리적 접근을 방지하기 위해 물리적 변조 방지 기능 (예. 잠금장치, 캡슐화, 보안 나사(비표준 헤드 유형))이 있어야 한다.
시험기준	불필요한 외부 인터페이스에 물리적 변조 방지 기능이 있어야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 물리적 변조 방지 기능을 확인한다. 2) 의료기기의 불필요한 외부 인터페이스에 물리적 잠금장치 등 물리적 변조 방지 기능이 있는지 확인한다. 3) 물리적 잠금장치 등 물리적 변조 방지 기능이 없는 외부 인터페이스로 접근 시 접근통제 기능이 있는지 확인한다.
적용 예외사항	소프트웨어 의료기기(SaMD)에는 적용하지 않는다.

□ SI-11 부트 프로세스 무결성 검증

구분	내용
세부 요구사항	의료기기는 사용하기 전에 의료기기의 부트와 런타임 프로세스에 필요한 펌웨어, 소프트웨어 및 설정 데이터의 무결성을 검증해야 한다. * 부트 프로세스 무결성 보충 설명 악의적인 공격자가 의료기기, 자산 또는 데이터에 접근할 수 있는 안전하지 않거나 유효하지 않은 운영 상태로 부트되지 않음을 보장하기 위해, 의료기기는 부트 프로세스 동안 의료기기의 펌웨어, 소프트웨어 및 설정 데이터의 무결성 검증을 수행해야 한다.
시험기준	사용 전 부트 프로세스 관련 펌웨어, 소프트웨어 및 설정 데이터에 대한 무결성 검증 기능이 정상 동작하여야 한다.
시험방법 (예시)	1) 설계 문서, 사용자 설명서 등에서 정의된 부트 프로세스에서 수행되는 무결성 점검 대상 소프트웨어 및 설정 데이터와 관련 기능을 확인한다. 2) 부트 프로세스 시 수행되는 무결성 점검 결과 기록 등을 통해 무결성 점검이 수행되는지 확인한다.
적용 예외사항	소프트웨어 의료기기(SaMD)에는 적용하지 않는다.

데이터 기밀성(DC, Data Confidentiality)

□ DC-01 정보에 대한 기밀성 보장

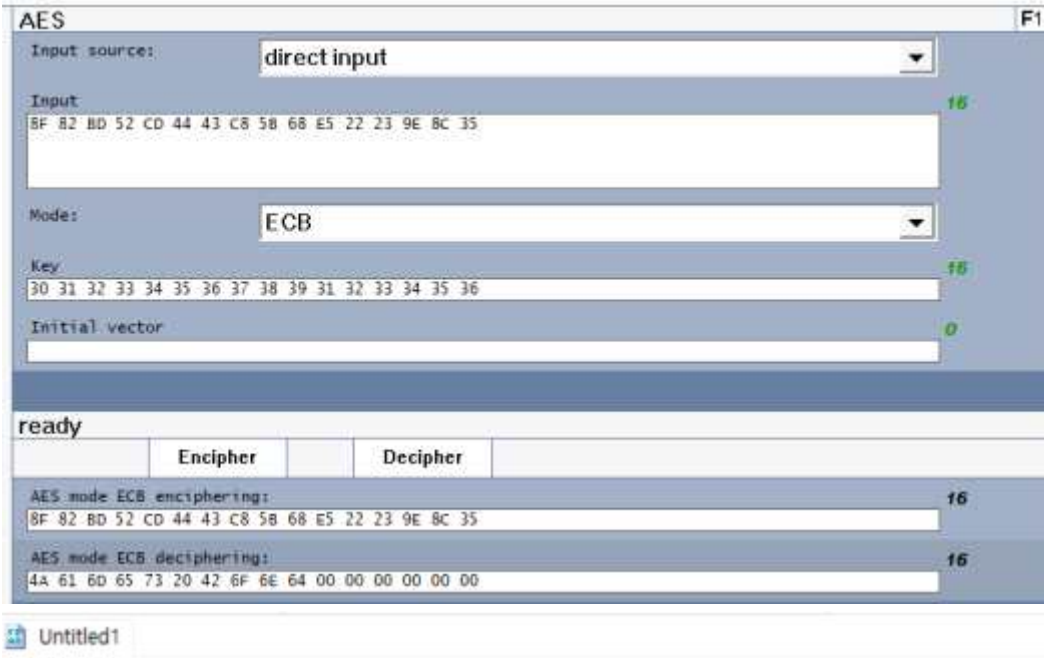
구분	내용
세부 요구사항	의료기기는 읽기 권한이 지원되는 저장 정보의 기밀성 보호 기능과 전송 중 정보의 기밀성 보호 기능이 있어야 한다.
시험기준	다음 사항을 모두 만족해야 하며, 정보에 대한 기밀성 보장 기능이 정상 동작하여야 한다. - 도청이나 우연한 노출을 통한 정보의 무단 공개로부터 보호하는 기능이 있다. - 읽기 권한이 지원되는 미사용 정보의 기밀성을 보호하는 기능이 있다. - 전송 중인 정보의 기밀성을 보호한다. - 암호화 통신(프로토콜)을 사용한다. - 오래되었거나 더 이상 사용되지 않는 프로토콜을 사용하지 않는다 - 추가 보호 기능(예. 암호화 서명)이 없는 평문 프로토콜(예. FTP)을 사용하지 않는다.
시험방법 (예시)	1) 의료기기에 접속하여 읽기 권한이 지정된 저장 정보가 암호화되었는지 확인한다. * Base64 수준의 인코딩이 적용되었거나 평문으로 저장되지 않아야 한다. 2) 읽기 권한이 지정된 정보가 의료기기에서 유·무선 방식으로 전송할 때, 네트워크 트래픽 모니터링 도구를 이용하여 네트워크 패킷을 덤프한다. 3) 덤프된 트래픽을 분석하여 암호화 여부를 확인한다. 4) 1번과 2번에서 적용된 암호 알고리즘의 보안강도를 확인한다. * DC-03로 해당 내용 확인 가능

□ DC-02 보건의료정보 비식별화

구분	내용
세부 요구사항	의료기기에 저장된 보건의료정보를 통해 권한이 없는 사람이 환자를 식별할 수 있는 경우, 해당 정보를 비식별화할 수 있는 기능(예. 애플리케이션 소프트웨어, 추가 도구 등)이 있어야 한다. * 참고사항 승인된 사용자만 접근할 수 있는 가명화 및 환자 식별 키를 사용하면, 승인된 사용자만 보건의료정보를 재식별화할 수 있다.
시험기준	보건의료정보 비식별화 기능을 통해 환자 식별정보를 알 수 없어야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등에서 정의된 보건의료정보 비식별화 기능을 확인한다. 2) 의료기기의 보건의료정보 비식별화 기능 또는 제조자가 비식별화 도구를 제공하는 경우, 해당 기능 또는 도구를 통해 보건의료정보를 정상적으로 비식별화 하는지 확인한다. - 저장된 보건의료정보와 비식별화된 결과를 확인하고, 비식별화에 사용된 비식별화 알고리즘을 확인 후 단방향 암호화 도구로 검증한다.  환자 전화번호: 0101113333 비식별화 (SHA256) 결과: D11DE51D998D05458752F7BEB42D537B61FC8494396C5C700FDC078D13F6BFB2 <보건의료정보 비식별화>
적용 예외사항	의료기기가 개인식별정보를 저장하지 않는 경우 적용하지 않는다.

□ DC-03 안전한 암호화 사용

구분	내용												
세부 요구사항	암호화가 필요한 경우, 의료기기는 국내·외에서 권고하는 암호학적 보안 기능을 사용해야 하며, 사용하는 암호화 키는 안전하게 관리하여야 한다.												
	* 보충 설명 암호학적 보호 적용 대상은 저장 정보나 전송 중 정보, 또는 양쪽 모두를 포함할 수 있다. 의료기기 공급자는 암호키 설정 및 관리와 관련된 사례와 절차를 문서화해야 한다. - AES, SHA 같은 검증된 암호 및 해시 알고리즘을 사용해야 한다. ※ 비밀번호는 Salt 값을 갖는 일방향 해시 알고리즘 적용 권고 - 표준 기반 키 길이(key size)를 활용해야 한다. - 키 생성은 효율적인 난수 생성기를 사용하여 수행해야 한다. - 키 관리의 보안 정책 및 절차는 정의된 표준에 따라 주기적인 키 변경, 키 폐기, 키 배포 및 암호키 백업을 다룰 필요가 있다.												
	* 국내·외 권고 암호 알고리즘 예시(112 비트 이상) <table><tr><th>구분</th><th>암호 알고리즘</th></tr><tr><td>대칭키 암호 알고리즘</td><td> • SEED, HIGHT • ARIA-128/192/256 • LEA-128/192/256 • AES-128/192/256 </td></tr><tr><td rowspan="2">해시 함수</td><td> 단순해시/ 전자서명용 • SHA-1 / HAS-160 ※ 80비트/112비트 보안강도를 제공하지 못하므로, 메시지 인증/키유도/난수생성용으로만 사용 가능함 • SHA-224/256/384/512 • SHA-512/224, SHA-512/256 • SHA3-224/256/384/512 • LSH-224/256/384/512 • LSH-512-224, SHA-512-256 </td></tr><tr><td> 메시지인증/ 키유도/ 난수생성용 </td></tr><tr><td rowspan="3">공개키 암호 알고리즘</td><td> 키 공유용 • [이산대수 문제] DH, MQV • [타원곡선] ECMQV, ECDH </td></tr><tr><td> 암·복호화용 • [인수분해 문제] RSAES, RSA </td></tr><tr><td> 전자서명용 • [인수분해 문제] RSA-PSS, RSA • [이산대수 문제] KCDSA, DSA • [타원곡선] ECDSA, EC-KCDSA, ECDSA </td></tr></table>		구분	암호 알고리즘	대칭키 암호 알고리즘	• SEED, HIGHT • ARIA-128/192/256 • LEA-128/192/256 • AES-128/192/256	해시 함수	단순해시/ 전자서명용 • SHA-1 / HAS-160 ※ 80비트/112비트 보안강도를 제공하지 못하므로, 메시지 인증/키유도/난수생성용으로만 사용 가능함 • SHA-224/256/384/512 • SHA-512/224, SHA-512/256 • SHA3-224/256/384/512 • LSH-224/256/384/512 • LSH-512-224, SHA-512-256	메시지인증/ 키유도/ 난수생성용	공개키 암호 알고리즘	키 공유용 • [이산대수 문제] DH, MQV • [타원곡선] ECMQV, ECDH	암·복호화용 • [인수분해 문제] RSAES, RSA	전자서명용 • [인수분해 문제] RSA-PSS, RSA • [이산대수 문제] KCDSA, DSA • [타원곡선] ECDSA, EC-KCDSA, ECDSA
	구분	암호 알고리즘											
	대칭키 암호 알고리즘	• SEED, HIGHT • ARIA-128/192/256 • LEA-128/192/256 • AES-128/192/256											
해시 함수	단순해시/ 전자서명용 • SHA-1 / HAS-160 ※ 80비트/112비트 보안강도를 제공하지 못하므로, 메시지 인증/키유도/난수생성용으로만 사용 가능함 • SHA-224/256/384/512 • SHA-512/224, SHA-512/256 • SHA3-224/256/384/512 • LSH-224/256/384/512 • LSH-512-224, SHA-512-256												
	메시지인증/ 키유도/ 난수생성용												
공개키 암호 알고리즘	키 공유용 • [이산대수 문제] DH, MQV • [타원곡선] ECMQV, ECDH												
	암·복호화용 • [인수분해 문제] RSAES, RSA												
	전자서명용 • [인수분해 문제] RSA-PSS, RSA • [이산대수 문제] KCDSA, DSA • [타원곡선] ECDSA, EC-KCDSA, ECDSA												
(출처) 암호 알고리즘 및 키 길이 이용 안내서, 한국인터넷진흥원(2018)													

시험기준	다음 사항을 모두 만족해야 한다. - 표준화된 암호 알고리즘을 사용한다. - 권장 프로토콜(예. KS X IEC 62443-4-2 CR 4.3에 언급된 기타 예시)을 사용한다.
시험방법 (예시)	1) 통신 무결성, 정보 기밀성을 위해 사용되는 암호화에 대해 표준화된 암호화 알고리즘과 권장 프로토콜인지 확인한다. - 제시된 암호 알고리즘에 대하여 시험도구를 이용하여 출력된 암호화 데이터와 복호화된 데이터를 입력하여 검증한다.  (암호 알고리즘 AES128 ECB, 평문 데이터: James Bond, 암호화 키: 0123456789123456, 암호화 결과: 8F 82 BD 52 CD 44 43 C8 5B 68 E5 22 23 9E 8C 35) <암호 알고리즘 검증> 2) 암호키에 대한 생성, 저장, 사용, 파괴 정책을 확인한다.

이벤트 적시 대응(TRE, Timely Response to Events)

☐ TRE-01 감사로그에 대한 비인가된 접근 제한

구분	내용
세부 요구사항	의료기기는 인가된 사용자만 읽기 전용으로 감사로그에 접근할 수 있다.
시험기준	권한이 있는 사용자만 읽기 전용으로 감사로그에 접근할 수 있어야 하며, 수정할 수 있는 기능이 없어야 한다.
시험방법 (예시)	1) 감사로그에 접근할 수 있는 권한을 가진 사용자와 접근 권한이 없는 사용자를 추가한다. 2) 권한이 부여된 사용자에게 의해서만 감사기록에 접근할 수 있는지 확인한다. 3) 권한이 부여된 사용자로 감사기록에 접근 시 감사기록을 수정할 수 있는 기능이 있는지 확인한다.

자원 가용성(RA, Resource Availability)

☐ RA-01 서비스 거부(Denial of Service, DoS) 방지

구분	내용
세부 요구사항	- 의료기기는 DoS 이벤트 중에도 필수 기능을 유지하는 기능이 있어야 한다. - DDoS의 경우 공용 네트워크망에 접속하여 의료기기를 실시간으로 제어 또는 환자 생명과 직접적으로 연관될 수 있는 정보를 실시간으로 송수신하는 장비에 적용하고, DDoS 공격에 대한 대응책이 수립되어야 한다.
시험기준	DoS 이벤트가 발생하는 동안 필수 기능이 정상 동작하여야 한다.
시험방법 (예시)	1) 시험자는 의료기기의 네트워크 인터페이스와 필수 기능을 식별한다. 2) 네트워크 패킷 생성 도구(예. STC) 또는 DoS 도구를 이용하여 의료기기 인터페이스로 DoS 공격을 수행한다. 3) DoS 공격 수행 시 의료기기의 필수 기능이 정상 동작하는지 확인한다.

□ RA-02 의료기기 백업

구분	내용
세부 요구사항	의료기기는 백업 기능이 있어야 하며, 백업 프로세스는 정상적인 의료기기 작동에 영향을 미치지 않아야 한다.
시험기준	다음 사항을 모두 만족해야 한다. - 의료기기에 대한 백업 기능이 정상 동작하여야 한다. - 백업 프로세스가 정상 작동에 영향을 미치지 않는다. - 백업 정보에 암호키 등 보호가 필요한 정보를 포함하는 경우, 민감한 데이터 암호화, 민감한 정보 제외 등과 같은 보호 기능이 정상 동작하여야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등을 확인하여 백업 기능과 백업 정보를 확인한다. 2) 의료기기 백업을 수행하여 정상적으로 백업이 되고, 백업이 수행되는 동안 의료기기 작동이 제한되거나 작동되지 않는 등의 영향을 미치는지 확인한다. * (선택) 백업 전·후의 자원 사용량을 확인하여 의료기기 작동에 영향을 미칠 가능성이 있는지 확인할 수도 있다. 3) 백업 정보에 보호가 필요한 정보가 포함되는 경우, 백업되는 일부 민감한 데이터에 대해 암호화 등과 같은 기능을 이용하여 데이터를 보호하고 있는지 확인한다.

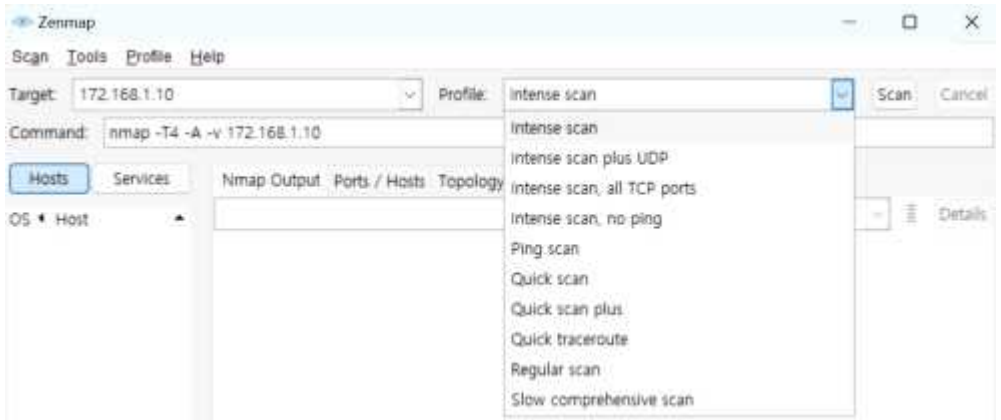
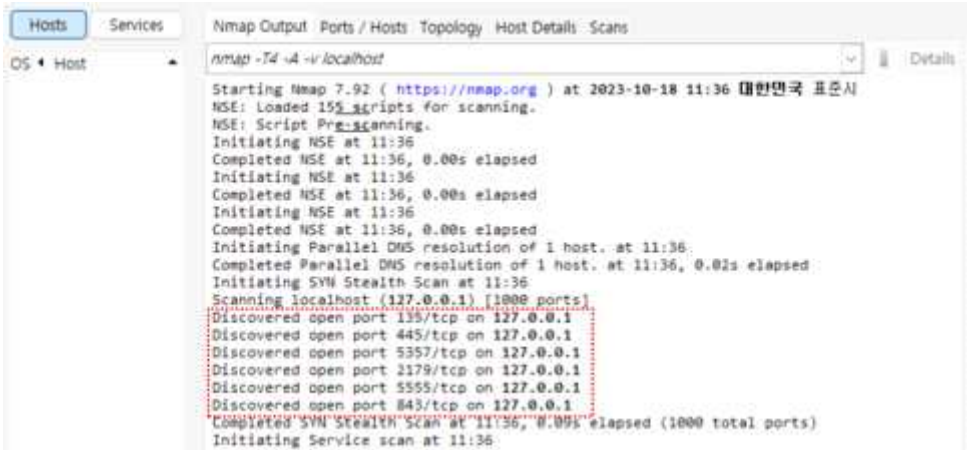
□ RA-03 의료기기 복구 및 재구성

구분	내용
세부 요구사항	의료기기는 중단 또는 장애 상황 발생 후 안전한 상태로 복구 및 재구성하는 기능이 있어야 한다.
시험기준	중단 또는 장애 후 보안 상태로 복구 및 재구성하는 기능이 있어야 하며, 다음 사항을 모두 만족해야 한다. - 시스템 매개변수(기본값 또는 설정 가능)는 안전한 상태로 구성할 수 있는 값으로 설정한다. - 보안에 중요한 패치가 다시 설치된다. - 보안 관련 구성 설정이 다시 설정된다. - 사용자 설명서 및 운영 절차를 사용할 수 있다. - 의료기기가 다시 설치되고 기존 설정으로 구성된다. - 권한 있는 사용자에게 의해 선택한 백업 또는 인증된 백업을 사용하여 복구한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등을 확인하여 중단 또는 장애 상황 정의를 확인하고, 중단 또는 장애 상황 발생 시 의료기기 복구 및 재구성 기능을 확인한다. 2) 의료기기 중단 또는 장애를 발생시킨다. 3) 의료기기가 안전한 상태로 복구 및 재구성되는지 확인한다.

□ RA-04 네트워크 및 보안 구성 설정

구분	내용
세부 요구사항	의료기기는 사용자 설명서에서 권고하는 네트워크와 보안 구성에 따른 설정 기능과 인터페이스가 있어야 하며, 구성 설정 변경을 모니터링하고 통제할 수 있어야 한다.
시험기준	다음 사항을 모두 만족해야 한다. - 사용자 설명서에 네트워크 및 보안 구성에 따른 설정 기능과 인터페이스에 대한 설명이 있으며, 해당 내용에 따라 네트워크 및 보안 구성을 설정할 수 있다. - 네트워크 및 보안 구성 설정 변경에 대한 모니터링 기능이 정상 동작한다.
시험방법 (예시)	1) 사용자 설명서를 확인하여 네트워크 및 보안 구성에 대한 인터페이스를 서술하고 있는지 확인한다. 2) 서술된 내용에 따라 네트워크와 보안 구성에 따른 설정 기능이 있는지 확인한다. 3) 해당 인터페이스를 통해 네트워크와 보안 구성에 대한 설정을 변경할 수 있는지, 권고된 구성으로 설정되어 있는지 확인한다. 4) 구성 설정 변경 시 이에 대한 감사기록 등 모니터링할 수 있는 기능이 있는지 확인한다.

□ RA-05 불필요한 기능 비활성화

구분	내용
세부 요구사항	의료기기는 불필요한 기능, 포트, 프로토콜, 서비스의 사용을 제한하는 기능(기본 구성 설정 이외의 기능은 비활성화)이 있어야 한다.
시험기준	불필요한 기능, 포트, 프로토콜 또는 서비스의 사용을 제한하는 기능이 정상 동작하여야 한다.
시험방법 (예시)	1) 의료기기 설계 문서, 사용자 설명서 등을 확인하여 의료기기가 기본적으로 제공하는 서비스(포트)를 식별하고 이에 대한 용도와 서비스(포트), 프로토콜, 기능을 비활성화하는 방법을 확인한다. 2) 포트 스캔 도구를 이용하여, 의료기기에서 열린 포트(서비스)를 확인한다. Zenmap을 실행하여 점검대상 의료기기의 IP(예. 172.168.1.10)를 입력하고, Intense scan plus UDP, Intense scan, all TCP ports 등을 선택하여 열린 포트를 확인한다.  3) 포트 스캔 도구의 결과를 기반으로 불필요한 포트(서비스)가 열려 있는지 확인한다. ① Zenmap을 실행결과에서 열린 포트(135, 445, 5357 등)를 다음과 같이 확인한다.  ② 의료기기 설계 문서, 사용자 문서 등에 해당 포트에 대한 사용 목적을 제시하고 있지 않은 포트가 있는지 확인한다.

	4) 의료기기가 제공하는 서비스(포트) 등의 비활성화 기능을 시험하여 포트 스캔 도구 등을 통해 정상적으로 서비스(포트) 등이 비활성화되었는지 확인한다. 3번 항목에서 불필요한 포트가 확인된 경우, 해당 포트를 기본적으로 비활성화되도록 수정하도록 하고, zenmap을 통해 재확인한다.
--	---

1. 제출 자료의 범위 및 요건

가. 제출 자료의 범위

유·무선 통신 경로가 있는 의료기기는 허가 신청 시 「의료기기 허가·신고·심사 등에 관한 규정」(식약처 고시) 제29조(첨부자료의 요건) 제8호 성능에 관한 자료 중 ‘소프트웨어 검증 및 유효성 확인 자료’와 ‘의료기기 소프트웨어 적합성 확인보고서’를 제출하여야 하며, 제출 시 정보의 위변조, 오작동 또는 의료기기에 승인되지 않은 접근 등으로부터 방지하기 위한 대책으로 표 2의 의료기기 사이버보안 요구사항을 적용하여야 한다.

제조자는 의료기기 사이버보안 요구사항에 대한 준수 여부를 확인할 수 있도록 표 3의 ‘의료기기 사이버보안 요구사항 체크리스트’와 체크리스트의 요구사항을 실제로 검증한 자료를 제출하여야 한다. 다만, 제조사의 위험분석을 통해 요구사항 일부를 제외하거나 수정하여 적용하는 경우에는 제26조 제1항 제4호에 따른 시험규격 및 그 설정근거를 제출하여야 하며, 해당 자료로 ‘사이버보안 위험관리문서’를 제출할 수 있다.

< 사이버보안 제출 자료 예시 >

1. 의료기기 사이버보안 요구사항 체크리스트

2. 사이버보안 요구사항을 검증한 자료

- 소프트웨어 검증 및 유효성 확인 자료
- 사이버보안 위험관리문서
- 성능시험성적서

3. 사이버보안 요구사항 미적용 근거를 확인할 수 있는 자료

- 사이버보안 위험관리문서 등

‘의료기기 사이버보안 요구사항 체크리스트’는 의료기기 사이버보안 요구사항에 대한 적합성 여부를 확인할 수 있는 자료로 의료기기 허가·심사 시 의료기기 사이버보안 요구사항 체크리스트 양식을 활용하여 제품의 특성에 맞게 작성하여 제출한다.

‘사이버보안 위험관리문서’와 ‘소프트웨어 검증 및 유효성 확인 자료’는 신청 제품이 의료기기 사이버보안 요구사항 체크리스트에 기재한 사이버보안 요구사항을 만족하고 있음을 확인할 수 있는 근거 자료이다.

‘사이버보안 위험관리문서’는 의료기기 전체 생명주기에서의 사이버보안과 관련된 위해요인을 파악하여 발생 가능한 위해를 최소화 및 차단하기 위한 위험관리 활동을 기록한 보고서로 신청 제품의 사이버보안과 관련된 위해요인 식별과 각 위해요인에 대한 위험분석 및 위험경감 조치의 결과를 기재하여야 한다.

‘소프트웨어 검증 및 유효성 확인 자료’는 의료기기의 위험관리 과정에서 식별된 위해요인에 대한 위험통제 조치의 결과를 검증할 수 있는 객관적인 자료로서 사이버보안 요구사항에 대한 시험 및 검증 절차, 시험결과, 시험 및 검증 도중 소프트웨어 변경이 발생한 경우 재시험 결과를 포함하여야 한다.

‘사이버보안 위험관리문서’와 ‘소프트웨어 검증 및 유효성 확인 자료’는 「의료기기의 사이버보안 적용방법 및 사례집(2022)」과 「의료기기 소프트웨어 허가·심사 가이드라인(2023)」을 참조하여 작성할 수 있다.

나. 제출 자료의 요건

사이버보안에 관한 자료는 아래 요건에 적합한 자료를 제출한다.

「의료기기 허가·신고·심사 등에 관한 규정」(식약처 고시) 제29조(첨부자료의 요건) 제8호 성능에 관한 자료

1. 식약처장이 지정한 시험검사기관에서 발급한 시험성적서
2. 대학 또는 연구기관 등 국내·외의 전문기관에서 시험한 것으로서 해당 기관의 장이 발급하고 그 내용(기관의 시험시설 개요, 주요설비, 연구인력 구성, 시험자의 연구경력 등을 포함한다)을 검토하여 타당하다고 인정할 수 있는 시험성적서
3. 「의료기기 제조 및 품질관리기준」(식품의약품안전처 고시)또는 이와 동등 이상의 규격에 따른 제조사의 품질관리시스템 하에서 실시한 제품의 성능에 관한 시험성적서

전문기관에서 시험한 자료는 한국인터넷진흥원(KISA)의 IoT 보안 인증 인증서(정보통신망연결기기 등 정보보호인증서) 등을 제출할 수 있으며, 해당 기관에서 발급한 인증서 및 시험결과를 확인할 수 있는 자료(결과요약서, 시험성적서 등)를 제출할 수 있다.

 인증서	 결과요약서
---	--

2. 의료기기 사이버보안 요구사항 체크리스트

의료기기 사이버보안 요구사항 체크리스트 작성 시 사용되는 통신 기술 (유·무선 통신 방식 등), 사용 환경(병원 내/외 사용, 공용 네트워크망 사용 등) 등의 통신 특성을 확인할 수 있는 사항을 기재한다.

이를 기반으로 하여 아래의 사이버보안 요구사항 체크리스트에 따라 요구사항 적용여부, 적합성 입증방법, 첨부자료 또는 문서번호를 기재한다.

신청 제품의 기술적 특성 상 요구사항이 제외 또는 추가될 수 있으며, 요구사항이 제외되는 경우 적절한 사유를 '적합성 입증 방법' 란에 기재하고, 추가되는 경우 사이버보안 요구사항에 추가 기재할 수 있다. 예를 들어, 소프트웨어 의료기기(SaMD)의 경우 하드웨어로만 구현할 수 있는 보안 요구사항은 제외할 수 있으며, 소프트웨어로 보안위협에 대해 통제 조치를 할 수 있는 경우 요구사항을 추가 기재할 수 있다.

[표 3. 의료기기 사이버보안 요구사항 체크리스트]

< 의료기기 사이버보안 특성 기재 >

- 1) 사용되는 통신 기술: 유선 통신(USB, RS-232, LAN), 무선 통신(Wi-Fi, 블루투스, RF 통신)
- 2) 사용 환경: 병원 내 사용, 병원 외 사용
- 3) 공용 네트워크망 사용여부: Y/N

사이버보안 요구사항			해당 기기 적용 여부	적합성 입증 방법	해당 첨부자료 또는 문서번호
식별 및 인증 (IA)	IA-01	사용자 식별 및 인증	적용 /미적용	사용자 로그인 (ID/PW) 기능 구현	문서번호, 페이지, 요구사항 ID, 시험항목 #
	IA-02	계정 관리			
	IA-03	식별정보 관리			
	IA-04	인증정보 관리			
	IA-05	비밀번호 강도 설정			
	IA-06	인증정보에 대한 피드백			
	IA-07	연속적인 로그인 시도 실패 시 로그인 제한			
	IA-08	시스템 사용 알림 메시지			
사용 통제 (UC)	UC-01	권한 부여			
	UC-02	모바일 코드 사용 통제			
	UC-03	세션 잠금			
	UC-04	감사기록 생성			
	UC-05	감사 처리 실패 대응			
	UC-06	타임스탬프			
	UC-07	부인 방지			

시스템 무결성 (SI)	SI-01	통신에 대한 무결성 보장			
	SI-02	악성코드로부터 보호			
	SI-03	보안 기능 검증			
	SI-04	소프트웨어 및 정보에 대한 무결성 점검			
	SI-05	입력값 검증			
	SI-06	오류 시 사전 결정된 상태로 출력			
	SI-07	오류 처리			
	SI-08	업데이트			
	SI-09	업데이트에 대한 진본성 및 무결성 검증			
	SI-10	물리적 변조 방지			
	SI-11	부트 프로세스 무결성 검증			
데이터 기밀성 (DC)	DC-01	정보에 대한 기밀성 보장			
	DC-02	보건의료정보 비식별화			
	DC-03	안전한 암호화 사용			
이벤트 적시 대응 (TRE)	TRE-01	감사로그에 대한 비인가된 접근 제한			
자원 가용성 (RA)	RA-01	서비스 거부(Denial of Service, DoS) 방지			
	RA-02	의료기기 백업			
	RA-03	의료기기 복구 및 재구성			
	RA-04	네트워크 및 보안 구성 설정			
	RA-05	불필요한 기능 비활성화			

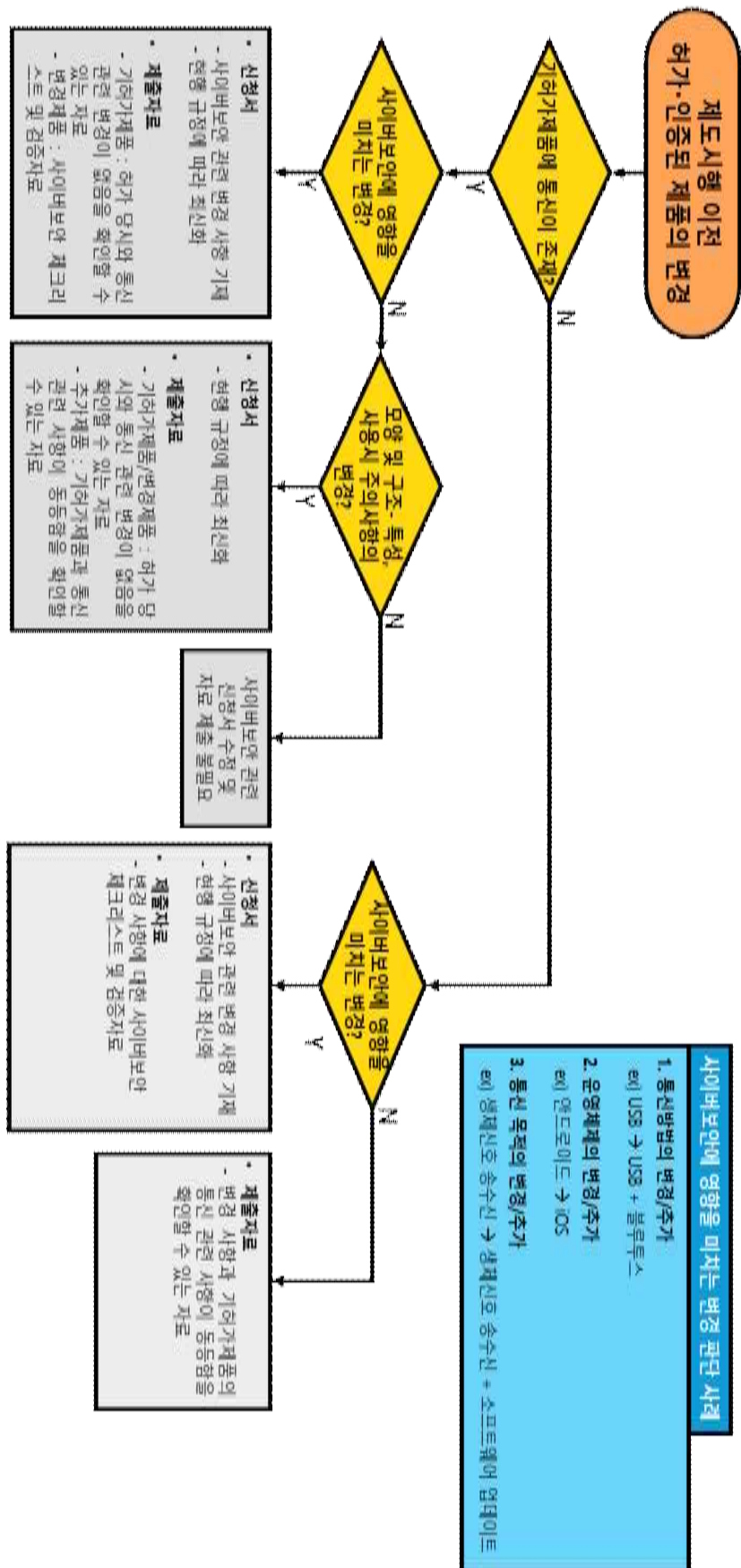
3. 허가인증 변경 시 제출자료

사이버보안에 영향을 미치는 변경(통신방법의 변경·추가, 운영체제의 변경·추가, 통신 목적 변경·추가 등)이 포함된 경우에는 「의료기기 허가·신고·심사 등에 관한 규정」(식약처 고시) 제19조의2(의료기기 소프트웨어 허가·인증·신고의 변경 처리), 「디지털의료제품법 시행규칙」 제19조(디지털의료기기 변경허가 등)에 따라 변경허가·인증·신고하여야 한다.

이 경우에는 신규 허가과 마찬가지로 ‘의료기기 소프트웨어 적합성 확인보고서’, ‘의료기기 사이버보안 요구사항 체크리스트’와 체크리스트의 요구사항을 실제로 검증 또는 검증을 대체한 사유를 확인할 수 있는 자료(소프트웨어 검증 및 유효성 확인자료, 성능시험성적서, 위험관리 문서 등)를 제출하여야 한다.

다만, 변경 사항과 기허가 제품의 통신 관련 사항이 동등함을 확인하는 자료(예: 제조원의 품질관리체계에서 관리되고 있는 제품 개발 및 설계 문서 등)를 제출하여 변경사항이 사이버보안에 영향을 미치지 않는 것으로 판단되는 경우에는 추가적인 자료 제출이 불필요하다.

또한, 의료기기 사이버보안 자료 의무 제출 제도 시행(‘19.11월) 이전 허가받은 제품의 경우에는 기허가 제품의 변경 신청일자 기준으로 최신 규정을 적용하여 신청내용을 기재하여야 하며, 통신 구성의 변경이 없더라도 현행 규정에 따라 ‘모양 및 구조-특성’에 통신구성도 및 ‘사용시 주의사항’에 사이버보안 사고 발생 시 대응 관련 문구 기재가 필요하다.



[그림 2. 허가·인증 변경 시 의료기기 사이버보안 관련 제출 자료 흐름도]

1. 보건의료기본법, 법률 제17966호, 보건복지부(2021)
2. 암호 알고리즘 및 키 길이 이용 안내서, 한국인터넷진흥원(2018)
2. 의료기기 소프트웨어 허가·심사 가이드라인, 식품의약품안전처(2023)
3. 의료기기 위험관리 가이드라인, 식품의약품안전처(2007)
4. 정보통신망연결기기등 정보보호인증기준 상세 해설서, 한국인터넷진흥원(2023)
5. Cybersecurity in Medical Devices Quality System Considerations and Content of Premarket Submissions, FDA(2023)
6. IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels
7. IEC 62443-4-1:2018, Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
8. IEC 62443-4-2:2019, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
9. IEC TR 60601-4-5:2021, Medical electrical equipment - Part 4-5: Guidance and interpretation - Safety-related technical security specifications
10. ISO 14971, Medical devices - Application of risk management to medical devices(2019)
11. KS X IEC 62443-3-3:2021, 산업 통신 네트워크 - 네트워크 및 시스템 보안 - 제3-3부: 시스템 보안 요구사항 및 보안 등급
12. KS X IEC 62443-4-1:2021, 산업제어시스템 보안 - 제4-1부: 안전한 제품 개발 생명주기 요구사항
13. KS X IEC 62443-4-2:2020, 산업제어시스템 보안 - 제4-2부: 산업제어시스템 컴포넌트의 기술적 보안 요구사항
14. Postmarket Management of Cybersecurity in Medical Devices, FDA(2016)
15. Principles and Practices for Medical Device Cybersecurity, IMDRF(2020)

표 4는 가이드라인 개정 전·후의 사이버보안 요구사항을 비교한 것이다. 가이드라인 개정 전 사이버보안 요구사항은 IMDRF ‘의료기기 사이버보안 원칙 및 지침’(Principles and Practices for Medical Device Cybersecurity, IMDRF(2020)) 5.1 보안 요구사항 및 아키텍처 디자인의 사이버보안 설계 원칙을 적용한 것으로, 개정 후 표 2의 요구사항과 부합한다. 제조자는 아래의 표를 참조하여 2025. 6. 30.까지 한시적으로 개정 전 요구사항을 적용한 검증 문서를 제출할 수 있다. 다만, 「디지털의료제품법」에 따른 디지털의료기기는 법 시행(2025. 1. 24.)에 맞춰 개정된 요구사항을 적용하고, ‘인공지능 보안’에 대해 추가 검증이 필요하다.

[표 4. 가이드라인 개정 전·후 사이버보안 요구사항 비교]

항목	IMDRF 사이버보안 요구사항	개정 전 상세 요구사항 예시		개정 후 요구사항	
보안통신	제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유무선 통신 등)하여야 할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등	[1] 통신 구성 제품의 위해도 및 사용 환경을 고려하여 통신을 구성하여야 한다. ※ 입증 예시: 제품의 통신 구성 및 방법을 확인할 수 있는 통신구성도, 사용자 설명서 등		RA-04	네트워크 및 보안 구성 설정
				RA-05	불필요한 기능 비활성화
	제조자는 내·외부의 모든 입력에 대한 유효성을 확인하는 설계 특성을 고려하여야 하며, 보안이 취약한 통신(예. 가정용 네트워크 혹은 기존 기기)만을 지원하는 기기 및 환경에서 이루어지는 통신도 고려한다.	[2] 접근통제 및 인증: 식별 및 인증에 기반하여 의료기기 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에	[2-1] 통신 시 인가된 기기 또는 네트워크를 인식할 수 있는 수단을 갖추어야 한다.	UC-02	모바일 코드 사용 통제
	제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송수신 방법을 고려하여야		[2-2] 의료기기 접속 인식: 비인가된 의료기기가 접속될 시 이를 인식하여 구분할 수 있어야 한다. [2-3] 비인가된 의료기기 접속 제한 비인가된 의료기기의 접속 시 접속을 제한할 수 있어야 한다.		
				SI-05	입력값 검증

항목	IMDRF 사이버보안 요구사항	개정 전 상세 요구사항 예시		개정 후 요구사항	
	한다. ※ 예: 기기/시스템 간 통신 시 상호인증방법, 암호화 필요 여부, 과거에 전송된 명령어 및 데이터의 비인가 반복에 대한 방지, 사전에 정의된 통신 종료 시점의 적절성 여부 등	따라 인가된 데이터에만 접근 가능해야 한다.	[2-4] 비인가된 네트워크 통신 차단: 비인가된 네 트워크 통신 접속을 제 한할 수 있어야 한다. [2-5] 원격접속 차단: 의료 기기가 의료기관의 서버에 접속할 수 있는 경우, 의료 기기 도난 시 해당 의료 기기가 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다. [2-6] 의료기기 인증 관리: 의료기기 인증의 유효기간을 설정할 수 있어야 하며 설정된 유효기간 만료 시 접근이 통제되어야 한다. [2-7] 자동세션종료: 설정된 시간 이후에는 의료기기 간의 통신 또는 접속이 종료되도록 한다.	UC-03 세션 잠금	
				SI-01 통신에 대한 무결성 보장	
데이터 보호	제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보안(secure)이 확보된 해시(hash)로 저장되어야함	[3] 의료기기 데이터 전송 또는 저장의 기밀성 및 무결성 보장: 통신을 이용하는 의료기기의 데이터를 전송하거나 저장하는 경우 적절한 암호화 및 복호화 방식을 활용하여	[3-1] 안전한 암호 알고리즘 사용: 데이터 전송 및 저장 시 사용되는 암호 알고리즘은 112비트 이상 보안강도를 가진 검증된 암호 알고리즘 또는 모듈을 사용하여야 한다. * 인증정보 RSA, DSA, SHA 등 * 데이터: AES 등	DC-01 정보에 대한 기밀성 보장	
			[3-2] 개인의료정보 저장 관리: 의료기관 외부에서 사용되는 측정기기 또는 게이트웨이에는 개인의료 정보를 저장하지 않는 것을 권고한다.	DC-02 보건의료정보 비식별화	
				DC-03 안전한 암호화 사용	

항목	IMDRF 사이버보안 요구사항	개정 전 상세 요구사항 예시		개정 후 요구사항	
		기밀성과 무결성을 보장하여야 한다.			
	제조자는 기밀성에 대한 위험 통제 수단이 요구 될 때, 통신 프로토콜의 컨트롤(control)/시퀀싱 (sequencing) 필드의 메시지를 보호하거나 암호 화의 키 관련 자료가 손상 되는 것을 방지하도록 고려하여야 한다.	[4] 안전한 암호키 사용: 암호화 시 사용되는 암호키는 안전하게 관리되어야 한다.		DC-03	안전한 암호화 사용
기기 무결성	제조자는 데이터 부인 방지 (non-repudiation)를 보장하기 위한 설계 특성이 필요한 지를 결정하기 위해 시스템 레벨에서의 아키텍처를 평가하여야 한다. ※ 예: 감사 로그 기록 기능 제공	[5] 데이터 감사를 위한 시스템 로그 기록: 사용자가 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등과 같은 로그가 기록 되어야 한다.		UC-04	감사기록 생성
				UC-05	감사 처리 실패 대응
				UC-06	타임스탬프
				UC-07	부인 방지
				TRE-01	감사로그에 대한 비인가된 접근 제한
	제조자는 기기 소프트웨어의 비인가된 변경과 같은 기기의 무결성에 대한 위험을 고려해야 한다.	[6] 의료기기의 정상 동작을 보장하기 위해 주요 실행파일 및 설정파일에 대한 무결성을 검증하여야 하며, 무결성 오류 발생 시 대응방안을 고려하여야 한다.		SI-03	보안 기능 검증
				SI-04	소프트웨어 및 정보에 대한 무결성 점검
				SI-11	부트 프로세스 무결성 검증
	제조자는 바이러스, 스파이 웨어, 랜섬웨어 등 기기 에서 실행될 수 있는 악성 코드를 막기 위해 안티 멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.	[7] 불필요한 서비스 제거 또는 비활성화: 불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 외부 접속 포트를 사용할 경우 비밀 번호 설정, IP 제한 등의 추가적인 보안 조치를 수행하여야 한다.		SI-02	악성코드로부터 보호
사용자 인증	제조자는 기기의 사용이 인증된 사용자이거나, 다른 역할의 사용자에게 사용권한을 부여를 허용 하거나, 응급상황에서 접근을 허용하는 사용자 접근통제에 대해 고려하 여야 한다. 추가적으로 동일한 자격증명은 기기와	[8] 접근통제 및 인증: 식별 및 인증에 기반하여 사용자 역할에 따른 접근	[8-1] 인가된 사용자를 인식 할 수 있는 ID/PW, 하드 웨어키, 생체인증 등의 수단을 갖추어야 한다. [8-1-1] 비밀번호를 사용하는 경우, 다음을 적용해야 한다. - 비밀번호 작성 규칙 강화 - 비밀번호 하드코드 금지	IA-01	사용자 식별 및 인증
				IA-02	계정 관리

항목	IMDRF 사이버보안 요구사항	개정 전 상세 요구사항 예시		개정 후 요구사항	
	고객들에게 공유되지 않아야 한다. ※ 접근통제의 예: 비밀번호, 하드웨어 키, 생체 인증 등	권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.	- 비밀번호 노출 금지 [8-2] 다중접속 금지: 동일 사용자가 다중으로 접속하지 않아야 한다. [8-3] 사용자 접속 인식: 비인가된 사용자가 접속될 시 이를 인식하여 구분할 수 있어야 한다. [8-4] 비인가된 사용자 접속 제한: 비인가된 사용자의 접속 시 접속을 제한할 수 있어야 한다. [8-5] 원격접속 차단: 사용자가 의료기관의 서버에 접속할 수 있는 경우, 사용자 계정 도난 시 해당 계정이 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다. [8-6] 사용자 인증 관리: 사용자 계정의 유효기간을 설정할 수 있어야 하며, 설정된 유효기간 만료 시 접근이 통제되어야 한다. [8-7] 자동세션종료: 설정된 시간 이후에는 사용자의 접속이 종료되도록 한다.	IA-03 IA-04 IA-05 IA-06 IA-07 UC-01	식별정보 관리 인증정보 관리 비밀번호 강도 설정 인증정보에 대한 피드백 연속적인 로그인 시도 실패 시 로그인 제한 권한 부여
소프트웨어 유지보수	제조자는 주기적인 업데이트의 구현과 배포를 위한 수행절차를 수립하고 통보하여야 한다. 제조자는 운영체제(OS) 소프트웨어, 제3자 소프트웨어, 오픈소스 소프트웨어가 업데이트나 통제될 경우에 대해 고려하여야 한다. 또한 제조자는 외부의 통제에 의한 소프트웨어의	[9] 펌웨어 또는 소프트웨어 업데이트의 인가: 펌웨어 또는 소프트웨어 업데이트 시 관리자의 인가를 요청 및 확인하는 절차가 있거나 관리자 또는 사용자가 인지할 수 있는 거리에서 보안이 보장되는 방법으로 수행되어야 한다.		SI-08	업데이트

항목	IMDRF 사이버보안 요구사항	개정 전 상세 요구사항 예시		개정 후 요구사항	
	업데이트나 운영환경 만료에 대한 대응 계획을 수립하여야 한다. ※ 예: 보안이 보장되지 않은(unsecure) 운영체제 버전에서 운영되는 의료기기 소프트웨어 제조자는 새로운 사이버보안 취약성에 대응할 의료기기 업데이트 방안을 고려하여야 한다. ※ 예: 업데이트 시 사용자 개입/ 자동 업데이트 여부, 기기의 안전(safety)과 성능에 영향을 보장할 수 있는 업데이트 유효성 검증				
	제조자는 업데이트의 수행하기 위해 어떤 연결이 필요한지와 코드 서명 및 기타 비슷한 수단을 통한 연결이나 업데이트의 진본성을 고려하여야 한다.	[10] 펌웨어 또는 소프트웨어 업데이트의 무결성 보장: 펌웨어 또는 소프트웨어 업데이트 파일 배포 시 버전 식별이 가능하여야 하며, 파일에 대한 배포자 및 무결성을 검증할 수 있어야 한다.	[10-1] 펌웨어 또는 소프트웨어 업데이트 시 인증 방식 사용: 펌웨어 또는 소프트웨어의 업데이트 시 코드 서명 정보를 사용하고 코드 서명 정보는 안전한 해시 코드로 보호하여야 한다.	SI-09	업데이트에 대한 진본성 및 무결성 검증
물리적 접근	제조자는 비인가된 개인이 의료기기에 접근하는 것을	[11] 물리적인 통신포트 침해의 최소화 - 통신포트의 침해를 최소화하기 위해		IA-08	시스템 사용 알림 메시지

항목	IMDRF 사이버보안 요구사항	개정 전 상세 요구사항 예시	개정 후 요구사항	
	방지하기 위한 통제수단을 고려하여야 한다. ※ 예: 물리적 잠금 혹은 포트(port) 접근의 물리적 제한, 인증이 필요없는 물리적 케이블의 접근 제한 등	기기에 물리적인 잠금을 제공하여야 한다.		
			SI-10	물리적 변조 방지
신뢰성 및 가용성	제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.	[12] 사이버보안 위협 탐지 시 취해야 할 대응책에 관한 정보 제공 - 의료기기의 사용 중 발생하는 사이버 보안 사고에 대하여 긴급 연락처 및 기기의 제조자와 상담을 할 수 있는 연락방식을 제공하 여야 하며, 사이버보안 위협 탐지 시 취해야 할 대응책을 수립하고 사용자 에게 제공하여야 한다. [13] DDoS 공격에 대한 방어 - 공용 네트워크망에 접속하여 의료기기를 실시간으로 제어 또는 환자 생명과 직접적으로 연관될 수 있는 정보를 실시간으로 송수신하는 장비의 경우 DDoS 공격에 대한 대응책이 수립되어야 한다.	UC-04	감사기록 생성
			SI-06	오류 시 사전 결정된 상태로 출력
			SI-07	오류 처리
			TRE-01	감사로그에 대한 비인가된 접근 제한
			RA-01	서비스 거부(Denial of Service, DoS) 방지
			RA-02	의료기기 백업
			RA-03	의료기기 복구 및 재구성

[전문가협의체 위원]

소속	직위	성명	비고
한남대학교	교수	이만희	학계
한국기계전기전자시험연구원	본부장	방지호	시험검사 기관/ 연구기관
한국기계전기전자시험연구원	센터장	정원석	
한국산업기술시험원	센터장	윤주신	
한국산업기술시험원	선임연구원	권이석	
한국인터넷진흥원	책임연구원	이상걸	
코어시큐리티(주)	부사장	한근희	산업계
삼성전자(주)	책임	김홍범	
(주)H3 시스템	대표	김민준	
(주)인바디	부장	김경근	
(주)루트로닉	상무이사	박치대	
(주)멕아이씨에스	프로	김도형	
(주)메디웨일	매니저	이다연	
(주)에이아이트릭스	매니저	이상준	
메드트로닉코리아(유)	대리	정유진	
보스톤사이언티픽코리아(주)	과장	김소영	
(주)필립스코리아	본부장	박소은	

의료기기의 사이버보안 허가·심사 가이드라인(민원인 안내서)

발행처	식품의약품안전처 식품의약품안전평가원
발행일	2025년 1월 10일
발행인	강석연
편집위원장	노혜원
편집위원	강영규, 신희정, 서혁준, 한영민, 배영우, 김미선, 김현수, 전상우, 서지원, 김종엽, 조예진, 김병남, 이진수, 김기나
	우) 28159 충북 청주시 흥덕구 오송읍 오송생명2로 187
문의처	식품의약품안전평가원 의료기기심사부 디지털헬스규제지원과
	전화: 043-719-3948 팩스: 043-719-3940

28159 충북 청주시 흥덕구 오송읍 오송생명2로 187
오송보건의료행정타운
식품의약품안전처 식품의약품안전평가원
의료기기심사부 디지털헬스규제지원과
TEL: 043)719-3948 FAX: 043)719-3940
<http://www.mfds.go.kr/medicaldevice>



[부패·공익신고 안내] ※ 신고자 및 신고내용은 보호됩니다.
▶ 식약처 홈페이지 “국민소통 > 신고센터 > 부패·공익신고 상담”코너



식품의약품안전처

식품의약품안전평가원