의료기기의 사이버 보안 적용방법 및 사례집(민원인 안내서)

2019. 11. 28

식품의약품안전처
식품의약품안전평가원
의 료 기 기 심 사 부

지침서 · 안내서 제 · 개정 점검표

명칭	의료기기의 사이버 보안 적용방법 및 사례집(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.

2019 년 11 월 28 일

담당자 손 승 호

확 인(부서장) 이 정 림

개정 이력서

의료기기의 사이버 보안 적용방법 및 사례집(민원인 안내서)

제 · 개정번호	승인일자	주요 내용
안내서-0996-01	2019.11.28	의료기기의 사이버 보안 적용방법 및 사례집(민원인 안내서) 제정

이 안내서는 의료기기의 허가·심사 시 사이버 보안의 적용방법 및 사례에 대하여 알기 쉽게 설명하거나 식품의약품안전처의 입장을 기술한 것입니다.

본 안내서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술방식('~하여야 한다' 등)에도 불구하고 민원인 여러분께서 반드시 준수하셔야 하는 사항이 아님을 알려드립니다. 또한, 본 안내서는 2019년 11 현재의 과학적·기술적 사실 및 유효한 법규를 토대로 작성되었으므로 이후 최신 개정법규 내용 및 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

※ "민원인 안내서"란 대내외적으로 법령 또는 고시·훈령·예규 등을 알기 쉽게 풀어서 설명하거나 특정한 사안에 대하여 식품의약품안전처의 입장을 기술하는 것(식품의약품안전처 지침서 등의 관리에 관한 규정 제2조)

1. 관련규정

(1) 「의료기기법」 제6조 (제조업의 허가 등)

(2) 「의료기기법」 제15조 (수입업허가 등)

(3) 「의료기기법」 시행규칙 제5조 (제조허가의 절차)

(4) 「의료기기법」 시행규칙 제6조 (제조인증의 절차)

(5) 「의료기기법」 시행규칙 제7조 (제조신고의 절차)

(6) 「의료기기법」 시행규칙 제8조 (시설과 제조 및 품질관리체계의 기준)

(7) 「의료기기법」 시행규칙 제9조 (기술문서 등의 심사)

(8) 「의료기기법」 시행규칙 제30조 (수입허가 신청 등)

(9) 「의료기기 허가·신고·심사 등에 관한 규정」

(10) 「의료기기 품목 및 품목별 등급에 관한 규정」

(11) 「의료기기 제조 및 품질관리 기준」

(12) 「의료기기의 전기·기계적 안전에 관한 공통기준규격」

2. 문의처

식품의약품안전처 식품의약품안전평가원 의료기기심사부 첨단의료기기과

전화 : (043) 719-3908

FAX : (043) 719-3900

목 차

Ⅰ 개요

1. 배경 및 목적

통신 기술을 이용한 의료기기 개발이 증가함에 따라 의료기기 해킹, 정보 유출 등 사이버 보안 위협의 사례가 증가하고 있다. 이러한 사이버 보안 위협은 의료기기의 오류와 결함을 야기하고, 환자 건강에 위해를 가할 수 있어 보안 위협에 대한 의료기기의 안전성 및 성능 확보가 필요하다.

최근 우리 처에서는 사이버 보안 위협에 대한 의료기기의 안전성 및 성능 확보를 위하여 「의료기기의 사이버 보안 허가·심사 가이드라인(민원인 안내서)」를 발간하였다. 동 가이드라인은 유·무선 통신이 가능한 의료기기에 대해 사용자의 건강에 직접적인 영향을 미칠 수 있는 사이버 보안 위협에 대하여 적용할 수 있는 최소한의 권고사항과 의료기기 허가·심사 시 제출해야 하는 자료의 범위를 제시하였다. 하지만 국내 의료기기 업체에서는 의료기기 사이버 보안 확보에 대한 인식과 대처가 미흡하고, 의료기기 허가 신청 시 사이버 보안과 관련된 첨부자료의 작성에 어려움이 있다.

이에 본 가이드라인에서는 의료기기 제조자가 의료기기 사이버 보안에 대한 안전성 및 성능을 체계적으로 확보하도록 사이버 보안 적용방법과 허가신청 시 제출하는 자료의 작성 예시를 제시하고자 한다.

2. 적용범위

가. 의료기기 사이버 보안 적용범위

의료기기의 허가·심사 시 사이버 보안이 요구되는 의료기기는 「의료기기의 사이버 보안 허가·심사 가이드라인(민원인 안내서)」에 따라 다음과 같다.

※의료기기의 사이버 보안 허가·심사 가이드라인(민원인 안내서)의 적용범위

본 가이드라인은 유·무선 통신이 가능한 의료기기의 사이버 보안 확보를 위한 것으로 다음 각 호의 어느 하나에 해당하는 의료기기에 적용한다.

1) 유·무선 통신을 이용하여 환자의 생체정보 등 개인의료정보를 송수신하는 의료기기
2) 유·무선 통신을 이용하여 기기를 제어할 수 있는 의료기기
3) 유·무선 통신을 이용하여 펌웨어 또는 소프트웨어 업데이트 등 유지보수하는 의료기기

나. 의료기기 허가·심사 시 첨부자료

유·무선 통신이 가능한 의료기기는 허가 신청 시「의료기기 허가·신고·심사 등에 관한 규정」(식약처 고시) 제29조(첨부자료의 요건)의 8. 성능에 관한 자료로서 '소프트웨어 검증 및 유효성 확인 자료'를 제출하여야 하며, 제출 시 정보의 위변조, 오작동 또는 의료기기에 승인되지 않은 접근 등으로부터 방지하기 위한 대책으로 의료기기 사이버 보안 요구사항을 적용하여 제출하여야 한다. 다만, 제조사의 위험분석을 통해 요구사항 일부를 제외하거나 수정하여 적용하는 경우에는 제26조 제1항 제4호에 따른 시험규격 및 그 설정근거를 제출하여야 하며 해당 자료로 '사이버 보안 위험관리문서'와 '의료기기 사이버 보안 필수원칙 체크리스트'를 제출할 수 있다.

Ⅱ 의료기기 사이버 보안 적용방법

1. 위험관리 보고서 적용방법

가. 위험관리 보고서 구성

의료기기 제조자는 「의료기기 제조 및 품질관리 기준」에 따라 의료기기와 관련된 위해요인을 식별하고 관련 위험을 산정, 평가 및 통제하며, 그 통제의 효율성을 모니터링하기 위한 절차를 수립하고 기록을 유지하여야 한다.

의료기기 사이버 보안 또한 동일한 위험관리 절차를 적용하여 사이버 보안 관점에서의 위해요인을 식별하고, 위험 분석, 평가, 통제 조치를 통해 사이버 보안 침해로 발생할 수 있는 환자의 위해를 경감시킬 수 있다. 이러한 일련의 사이버 보안 위험관리 절차들은 위험관리 보고서에 기록되어야 하며, 의료기기 허가·심사 시 사이버 보안 준수 여부를 검토하기 위해 위험관리 보고서가 제출되어야 한다.

의료기기 사이버 보안을 위한 위험관리 보고서는 일반적인 의료기기 위험관리 보고서의 일부분으로 구성하거나, 별도의 위험관리 문서로 작성할 수 있다. 다만, 동일한 위험관리 절차를 적용하기 때문에 사이버 보안을 위한 위험관리 보고서의 구성항목은 동일할 수 있다.

본 안내서에서는 위험관리 보고서의 구성항목 중 의료기기 사이버 보안 측면에서 추가적인 고려가 필요한 항목에 대해 위험관리 보고서 작성방법 및 ‘2등급 유헬스케어 게이트웨이’, ‘범용초음파영상진단장치’, ‘환자감시장치’의 3가지 품목에 대한 예시를 제시하고자 한다.

작성방법에서 기술하는 항목은 표 1과 같이 위험관리 보고서의 전체 작성항목 중, ‘용어의 정의, 제품설명, 위험분석, 위험평가, 위험통제, 전체 잔여위험 허용가능성 평가, FMEA 보고서’이며, 본 안내서에서 기재되지 않은 항목은 일반적인 위험관리 보고서 작성방법에 따라 기재하도록 한다.

또한, 위험관리 보고서 작성예시는 각 품목에 대한 특정 시나리오에 대해 작성한 것으로, 신청 제품의 기술적 특성, 통신 시나리오를 반영하여 위험관리 보고서를 작성 할 수 있다.

[표 1. '의료기기 사이버 보안을 위한 위험관리 보고서'의 구성항목 및 안내서의 작성방법 기재항목]

번호	항 목	구 성 요 소
1	개요 및 소개	- 해당 품목에 대한 일반적인 사항, 작성목적, 위험관리 관련 문서에 대해 기술
2	용어의 정의	- 의료기기 위험관리 시 적용된 주요 용어를 정리
3	제품 설명	- 제품이 사용하는 통신목적 및 통신사양, 운영환경, 보안특성 등 의료기기 사이버 보안과 관련된 제품의 특성 기재
4	위험분석 흐름도	- ISO 14971에 따른 위험분석 흐름도 기재
5	위험분석	- 의료기기 위험관리 프로세스 수행에 따른 인원, 조직 및 일자 - 사이버 보안과 관련된 위해요인 식별 - 각 위해 상황에서의 위험 산정
6	위험평가	- 식별 된 각 위해요인에 대하여 위험관리 계획서에 정의된 위험허용기준을 사용하여 위험 감소가 필요한지 결정
7	위험통제	- 위험감소가 요구되는 경우 위험통제활동을 수행하고 기록
8	전체 잔여위험 허용가능성 평가	- 식별된 전체 잔여위험의 허용가능성 여부 결정
9	위험관리보고서	- 위험관리절차의 최종 검토결과 요약
10	생산 및 생산 후 정보 입수를 위한 방법	- 생산 및 생산 후 단계에서 해당 의료기기 또는 유사 의료기기에 관한 정보를 수집하여 기록
11	FMEA 보고서	- 제품 설계 및 공정에서 발생될 수 있는 잠재적인 고장모드와 그 영향을 도표와 목록으로 확인할 수 있도록 제시

나. 위험관리 보고서 적용방법

1) 용어의 정의

○ 의료기기 위험관리 내에서 사용되는 일반적인 위험관리 용어 및 사이버 보안과 관련된 용어를 정리하고, 이에 대한 정의를 설명하여 이해의 오류를 최소화하도록 기재한다.

* ‘Ⅲ.1. 위험관리 보고서 적용사례’의 사례 참조

2) 제품 설명

○ 위험관리 활동에서 논의된 일반적인 제품의 특성과 함께 통신목적 및 통신사양, 보안특성, 제품의 운영환경 등 의료기기 사이버 보안과 관련된 기술적 사항을 기재한다.

○ 일반적인 제품의 특성으로는 ‘모양 및 구조, 원재료, 성능, 사용방법’ 등이 있으며, 동 안내서의 예시에서는 생략한다.

* ‘Ⅲ.1. 위험관리 보고서 적용사례’의 사례 참조

3) 위험분석(Risk analysis)

○ 위험분석에서는 ‘제품의 설명, 위험관리 절차에 참여한 인원, 조직, 일자, 의료기기의 의도된 용도와 특성 식별, 위해요인 식별, 위험산정’으로 구분하여 기재한다.

○ ‘제품의 설명, 위험관리 절차에 참여한 인원, 조직, 일자, 의료기기의 의도된 용도와 특성 식별’ 단계는 일반적인 위험관리 보고서 작성 방법에 따르며, 동 안내서의 예시에서는 생략한다.

○ ‘위해요인 식별’에서는 관련 자료(규격, 가이드라인, 국내·외 이상사례 등)에 근거하여 의료기기의 정상 및 고장상태에서 이미 알고

있거나 예측 가능한 의료기기 사이버 보안 측면의 위해요인들에 대하여 기록한다.

○ ‘위험산정’에서는 위해상황을 초래할 수 있는 예측 가능한 사건들을 조합하여 각 위해요인에 대한 위험을 산정한다.

○ 사용하는 위험분석 양식은 다음과 같으며, 반드시 이 양식을 따라야 하는 것은 아니다.

< 위해요인의 식별 >

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료

< 각 위해 상황에서의 위험산정 >

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성

* ‘Ⅲ.1. 위험관리 보고서 적용사례’의 사례 참조

4) 위험평가(Risk evaluation)

○ 식별된 각 위해요인에 대하여 위험관리 계획서에 정의된 위험허용 기준을 사용하여 위험 감소가 필요한지 결정한다.

○ 식별된 모든 위험에 대하여 위험에 대하여 위험의 평가 결과를 ‘위험을 허용할 수 없는 영역(Unacceptable)’과 ‘합리적으로 실현할 수 있는 가장 낮은 영역(ALARP)’, ‘허용할 수 있는 영역(Acceptable)’의 3단계 또는 ‘위험을 허용할 수 없는 영역(Unacceptable)’과 ‘허용할 수 있는 영역(Acceptable)’의 2단계로 구분 할 수 있다.

○ 동 안내서의 예시에서는 위험의 평가 결과를 ‘위험을 허용할 수 없는 영역(Unacceptable)’과 ‘합리적으로 실현할 수 있는 가장 낮은 영역(ALARP)’, ‘허용할 수 있는 영역(Acceptable)’의 3단계로 구분하여 작성하였다.

○ 사용하는 위험평가 양식은 다음과 같으며, 반드시 이 양식을 따라야 하는 것은 아니다.

No.	위험분석(Risk analysis)						위험평가 (Risk evaluation)	
	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성	위험	결과

* ‘Ⅲ.1. 위험관리 보고서 적용사례’의 사례 참조

5) 위험통제(Risk control)

○ 제조자는 위험평가 결과 중 위험을 허용 가능한 수준까지 감소시키기 위하여 위험통제 조치를 식별하고, 위험통제 활동을 수행하여야 한다.

○ 위험통제 단계에서는 위험통제 조치방법, 위험통제조치의 실행, 잔여위험 평가, 위험/이득 분석, 위험통제조치로부터 추가적으로 발생하는 위험, 위험통제의 완료 등의 내용을 포함하여야 한다.

○ 사용하는 위험통제 양식은 다음과 같으며, 반드시 이 양식을 따라야 하는 것은 아니다.

No.	위험통제 조치 (Risk Control)	위험통제 조치 실행	잔여위험평가			결과	위험/이득분석	추가발생위험	통제완료
			발생가능성	심각성	위험				

* ‘Ⅲ.1. 위험관리 보고서 적용사례’의 사례 참조

6) 전체 잔여위험 허용가능성 평가

○ 모든 위험통제조치가 실시되고 검증된 후 위험관리 계획에서 정의된 위험허용기준을 사용하여 해당 의료기기에서 식별된 전체 잔여위험이 허용가능한지 여부를 결정하고 기록한다.

○ 사용하는 전체 잔여위험 허용가능성 평가 양식은 다음과 같으며, 반드시 이 양식을 따라야 하는 것은 아니다.

No.	잔여 위험평가			결과	위험/이득 분석	추가 발생 위험	통제 완료	전체 잔여위험 허용가능성 평가 (Evaluation of overall residual risk acceptability)
	발생 가능성	심각성	위험					허용가능/허용불가

* 'Ⅲ1. 위험관리 보고서 적용사례'의 사례 참조

7) FMEA(Failure Mode and Effects Analysis) 보고서

○ 제품 설계 및 공정에서 발생될 수 있는 잠재적인 고장모드와 그 영향을 도표와 목록으로 확인할 수 있도록 기재한다.

○ 사용하는 FMEA 보고서 양식은 다음과 같으며, 반드시 이 양식을 따라야 하는 것은 아니다.

No.	위험분석 (Risk analysis)						위험 평가 (Risk evaluation)		위험통제 (Risk control)								전체 잔여위험 허용가능성 평가
	위해 요인	발생 가능한 사례	위해상황	위해	발생가능성	심각성	위험	결과	위험통제조치	위험통제조치 실행	발생가능성	심각성	위험	결과	위험/이득분석	추가발생위험	통제완료	허용가능 / 허용불가

* 'Ⅲ.1. 위험관리 보고서 적용사례'의 사례 참조

2. 필수원칙 체크리스트 적용방법

의료기기 사이버 보안 필수원칙 체크리스트는 「의료기기의 사이버 보안 허가심사 가이드라인」의 요구사항이 개발 제품에 적용됨을 점검하는 것으로 제조자는 체크리스트의 질의 사항을 확인하여 요구사항의 적용여부 등을 확인할 수 있다.

각 의료기기의 보안 필수원칙의 적용여부는 제품에 통신 기술의 적용여부, 적용 된 통신 기술 및 목적 등에 따라 판단 될 수 있다. 따라서 각 제품의 보안 특성을 아래 체크리스트 양식을 이용하여 기술한다.

[표 2. 의료기기 사이버 보안 안전성 등급 분류]

의료기기 사이버 보안 안전성 등급	정 의
상(major)	의료기기 사이버 보안 침해로 인해 사용자의 심각한 상해 또는 사망, 신체기능의 영구적 장애, 신체구조의 영구적 손상의 가능성이 있음
중(moderate)	의료기기 사이버 보안 침해로 인해 사용자의 일시적이고 경미한 상해, 의학적 중재가 필요할 수 있음
하(minor)	의료기기 사이버 보안 침해로 인해 사용자의 일시적인 불편, 의학적 중재 없이 가역적이거나 경미하고 단시간의 불편이 있을 수 있음

안전성 등급은 위 표에 따라 상, 중, 하 중 해당 되는 것을 체크한다. 통신 기술은 무선과 유선, 근거리와 원거리 등으로 구분되고 세부적으로 블루투스, Wi-Fi, LAN 등이 있어 해당 제품에 적용되는 것을 기술한다. 그리고 원격진료, 의료기기 간 정보 교환, 의료기기의 유지보수 등 통신 기술의 사용목적에 따라 통신의 사용 빈도 등이 달라 질 수 있고 이는 위험관리에 주요한 요소가 될 수 있다. 따라서 통신목적, 공용 네트워크망의

사용여부 등을 아래 체크리스트를 이용하여 기술한다.

< 의료기기 사이버 보안 특성 기재 >

1) 사이버 보안 안전성 등급 : □상 □중 □하

2) 사용되는 통신 기술 :

3) 통신목적 : □ 환자의 생체정보 등의 개인의료정보 송수신

□ 기기제어

□ 펌웨어 또는 소프트웨어 업데이트 등 유지보수

4) 공용 네트워크망 사용여부 :

「의료기기의 사이버 보안 허가심사 가이드라인」에 제시되어 있는 사이버 보안 필수원칙은 다음과 같이 해당기기 적용여부, 적합성 입증 방법, 해당 법규 및 규격, 해당 첨부자료 또는 문서번호로 구성된다.

의료기기의 보안 특성, 위험관리의 위험분석, 통제조치 등의 자료를 기반으로 '사이버 보안 필수원칙'의 각 항목의 적용여부를 체크한다. 필수원칙 적용되는 항목의 경우 적합성 입증 방법, 법규 및 규격, 이를 확인할 수 있는 첨부자료 또는 문서번호를 기재한다. 요구사항이 적용되지 않는 경우 적절한 사유를 '적합성 입증 방법' 란에 기재한다.

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1. 식별 및 보호				
1.1 접근통제 및 인증 식별 및 인증에 기반하여 사용자(의료기기) 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.				
1.2 다중접속 금지 동일 사용자가 다중으로 접속하지 않아야 한다.				
…	…	…	…	…

Ⅲ 의료기기 사이버 보안 적용사례

1. 위험관리 보고서 적용사례

아래는 ‘2등급 유헬스케어 게이트웨이’, ‘범용초음파영상진단장치’, ‘환자감시장치’의 사이버 보안을 위한 위험관리 보고서 적용사례이다.

해당 예시는 각 품목에 대한 특정 시나리오에 대해 작성한 것으로 반드시 이를 따라야 하는 것은 아니며, 제품의 특성에 따라 각 항목의 내용이 달라질 수 있다.

가. 2등급 유헬스케어 게이트웨이

1. 개요 및 소개

※ 개요 및 소개는 본 예시에서 생략한다.

2. 용어 정의

본 보고서에서 사용하는 주요 용어의 정의는 다음과 같다.

2.1 사이버 보안(Cybersecurity) : 사이버 공간에서의 정보의 기밀성, 가용성, 무결성을 보존하는 것

2.2 의료기기 사이버 보안 : 유·무선 통신을 통해 의료기기에 저장되거나 송수신되는 개인의료정보 또는 기기를 제어하기 위한 프로그램을 무단사용, 사용거부, 오용, 변경, 승인되지 않은 접근을 방지하도록 하는 대책

2.3 기밀성(Confidentiality) : 개인의료정보가 허가되지 않은 사람에게 공개되거나, 허가되지 않은 용도로 사용되지 않게 하는 기능

2.4 가용성(Availability) : 개인의료정보가 승인된 사용자에게는 즉시 제공되어야 하며, 필요한 때에 필요한 곳에서 필요한 형태로 존재하도록 하는 기능

2.5 무결성(Integrity) : 개인의료정보가 허가되지 않은 방법으로 변환되거나 파괴되지 않도록 하는 기능

2.6 암호화(Encryption) : 정보보안을 유지하기 위하여 그 정보를 특정한 규칙에 따라 변형하여 저장함으로써 해독방법을 모르면 그 정보의 내용을 알아볼 수 없도록 하는 기술

2.7 SSL : 웹브라우저와 웹서버 간에 안전하게 데이터를 송수신하기 위하여 암호화 가능을 제공하는 표준 보안 프로토콜

2.8 접근통제(Access control) : 정보 보안 정책에 따라 사용자, 프로그램, 프로세서, 시스템 등을 허가된 주체만이 정보 시스템 자원에 접근할 수 있도록 제한하는 것

2.9 BLE(Bluetooth low energy) : 배터리가 제한적인 소형 디바이스에 알맞게 전력이 적게 소모되도록 설계된 근거리 무선 통신기술

2.10 IT-네트워크(IT-Network) : 두 개 이상의 통신 노드 간의 물리적 연결 또는 무선 전송을 제공하기 위한 통신 노드와 전송 링크로 구성된 시스템

2.11 보안 취약점(Security vulnerability) : 시스템 또는 프로그램에 내재되어 있는 버그(잘못된 부분)를 의미하며, 해커는 이를 악용하여 시스템에 침입하고 정보 유출, 시스템 파괴 등 유발

2.12 DDoS : 여러 대의 공격자를 분산적으로 배치해 동시에 서비스 거부 공격을 하는 방법

2.13 위변조 : 위조(보안공격의 하나로 비인가자들이 시스템에 대한 위조물을 삽입하는 것)와 변조(보안공격의 하나로 비인가자들의 불법적인 접근뿐만 아니라 불법적인 변경 행위)를 아울러 이르는 말

2.14 위해(Harm) : 물리적인 상해나 손상 또는 재산이나 환경상의 손상

2.15 위해요인(Hazard) : 위해의 잠재적인 원인

2.16 위해상황(Hazardous situation) : 사람, 재산 또는 환경이 하나이상의 위해요인에 노출된 상태

2.17 의도된 용도(Intended use) : 제조자가 제공하는 사양, 지시서 및 정보에 따라 의도된 제품, 프로세스 또는 서비스의 사용

2.18 수명주기(Life-cycle) : 최초 개발단계에서 최종 폐기까지 의료기기 수명 모든 단계

2.19 위험(Risk) : 위해의 심각성과 발생가능성의 곱의 조합비율

2.20 위험분석(Risk analysis) : 위해요인을 식별하고 위험을 산정하기 위해 가용정보를 체계적으로 사용하는 것

2.21 위험통제(Risk control) : 위험을 규정된 수준 이하로 감소시키거나 유지하도록 하는 결정과 조치가 이루어지는 과정

2.22 위험산정(Risk estimation) : 위해요인의 발생가능성과 심각성의 값을 정하기 위해 사용되는 과정

2.23 위험평가(Risk evaluation) : 위험의 허용가능성을 결정하기 위해, 정해진 위험기준과 산정된 위험을 비교하는 과정

2.24 잔여위험(Residual risk) : 위험통제조치가 적용된 후에도 남아 있는 위험

2.25 전체 잔여위험 허용가능성 평가(Evaluation of overall residual risk acceptability) : 모든 위험통제조치가 이행되고 검증된 후, 위험관리계획에서 정의된 기준을 활용하여 해당 의료기기에서 제기된 전체 잔여위험이 허용 가능한 지 여부를 결정하는 과정

2.26 위험관리 파일(Risk management file) : 위험관리 프로세스에서 생성되는 것으로서 일련의 기록 및 기타 문서

2.27 안전성(Safety) : 수락 불가능한 위험으로부터 자유

2.28 심각성(Severity) : 위해요인으로 인해 발생 가능한 결과들의 정도

2.29 독립형 소프트웨어(Standalone Software) : 소프트웨어 그 자체로서 의료기기의 사용 목적에 부합하는 기능을 가지며, 범용 컴퓨터와 동등 환경에서 운영되는 의료기기 소프트웨어

<이하 생략>

3. 제품 설명

※ 모양 및 구조, 원재료, 제조방법, 사용방법, 사용 시 주의사항, 포장단위, 저장방법 및 사용기간, 시험규격 등 일반적인 제품의 사항은 본 예시에서 생략한다.

3.1 제품명

. **품 목 명** : 2등급 유헬스케어 게이트웨이
. **품목분류번호** : A90010.02
. **등 급** : 2등급
. **모 델 명** : MFDS1

3.2 사용목적 : 원격 진료(원격 모니터링)을 위해 유헬스케어 혈압계로부터 BLE 무선기술을 통해 혈압값을 수집·조회 및 분석하거나 감시하고 수집된 생체정보를 암호화하여 의료기관으로 전송하는 소프트웨어(모바일 의료용 앱)

3.3 사용환경 : 가정

3.4 소프트웨어 운영환경

- 독립형 소프트웨어
- 안드로이드 OS 버전 4.3 이상, Bluetooth Low Energy 통신 기능이 있는 단말기
- iOS 버전 9.1 이상, Bluetooth Low Energy 통신 기능이 있는 단말기

<2등급 유헬스케어 게이트웨이 통신 구성도>

3.5 통신목적

- 유헬스케어 혈압계와 2등급 유헬스케어 게이트웨이 : 원격진료를 위해 생체신호(혈압값)수신
- 2등급 유헬스케어 게이트웨이와 유헬스케어진단지원시스템 : 원격진료를 위해 생체신호(혈압값) 송신, 환자식별정보, 처방정보 등 진료정보 송수신
- 2등급 유헬스케어 게이트웨이와 제조원 서버 : 소프트웨어 업데이트 등 유지보수

3.6 통신시나리오

- 안드로이드 X.X을 사용하는 스마트폰에 설치되어 작동하는 어플리케이션
- 유헬스케어 게이트웨이는 의료기관 이외의 장소에서 인터넷 망을 이용하여 생체신호, 환자식별정보, 업데이트 정보 등을 송수신 함
- 생체신호 등은 본 제품에 임시저장하나 유헬스케어 진단지원시스템으로 전송 시 삭제하고 사용자가 게이트웨이를 통해 정보 조회 시 유헬스케어 진단지원시스템에서 조회

3.7 통신사양

- 유헬스케어 혈압계와 2등급 유헬스케어 게이트웨이 간 통신 : Bluetooth Low Energy
- 2등급 유헬스케어 게이트웨이와 유헬스케어 진단지원시스템 간 통신 : 3G, LTE, WiFi 통신

3.8 보안특성

- 유헬스케어 혈압계[2]와 2등급 유헬스케어 게이트웨이[2] 간 통신 : Bluetooth pairing
- 2등급 유헬스케어 게이트웨이[2]와 유헬스케어 진단지원시스템[3] 간 통신 : SSL 암호화

4. 위험분석 흐름도

※ 위험분석 흐름도는 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

5. 위험분석

5.1 위해요인의 식별

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
UH-01	비인가 접근	게이트웨이 정보에 비인가 접근으로 인한 환자 정보 조작	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	미 FDA Recall/ 체크리스트 1.1~1.11

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
UH-02		비인가자의 불법 소프트웨어 설치나 실행으로 게이트웨이의 오작동	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	미 FDA Recall/ 체크리스트 1.19
UH-03	정보 위변조	전송 정보(제어, 의료정보)의 유출 및 위변조	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트1.15/ 1.16/1.17
UH-04		게이트웨이에 저장된 정보의 위변조	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트 1.17/1.20
UH-05		비인가자가 게이트웨이에 저장된 정보를 위변조하여 진단지원시스템으로 전송	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트 1.17/1.20
UH-06		게이트웨이에 저장 된 정보가 알 수 없는 방법으로 암호화 된 경우	치료기회 박탈	미 FDA Recall
UH-07	플래폼 또는 하드웨어 취약	무허가 업데이트	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기 이상사례보고 / 체크리스트 1.12
UH-08		무결성이 보장되지 않은 업데이트	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기 이상사례보고 / 체크리스트 1.13
UH-09		인증되지 않은 업데이트	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기 이상사례보고 / 체크리스트 1.14
UH-10		시스템 로그 부재	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기 이상사례보고 / 체크리스트 2.1
UH-11		무결성이 보장되지 않은 실행파일 및 설정파일	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기 이상사례보고 / 체크리스트 2.2
UH-12		사이버 보안 위협 탐지 시 대응책 부재	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기 이상사례보고 / 체크리스트 2.3
UH-13	통신채널 취약	통신 서비스 거부, 통신 지연 등	진료 기회 박탈	의료기기 이상사례보고 / 체크리스트 2.3

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
UH-14				
UH-15				
UH-16				
UH-17				
…	…	…	…	…

※ 관련 자료 중 미 FDA Recall은 해당 제품 또는 유사 제품의 국외 Recall 사례를 의미함
※ '5.1 위해요인의 식별'의 위해요인에 대한 구체적인 예시를 아래 '5.2 각 위해 상황에서의 위험 산정' 시 위해요인으로 활용하여 위험을 산정한다.

5.2 각 위해 상황에서의 위험 산정

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
UH-01-01	게이트웨이 정보에 비인가 접근으로 인한 환자 정보 조작	사용자 구분을 하지 않고 누구나 환자의 정보에 접근하도록 한 경우	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	3	2
UH-01-02		하나의 계정에 여러 사용자가 동시에 접속한 경우, 데이터의 왜곡 발생	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01-03		비인가자의 접속 시도를 감지하지 못하는 경우	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01-04		보안이 취약한 공유기(Wi-Fi) 이용으로 사용자 접근 권한이 탈취된 경우	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01-05		도난된 정상 사용자 계정으로 원격에서 서버에 접속	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01-06		사용 유효기간이 경과(퇴사, 장기 출장 등)한 사용자 계정으로 기기 접속	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01-07		사용자가 자리를 비웠을 때 세션이 종료되지 않은 계정에 비인가자가 이용	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
UH-01 -08		로그인 시 비밀번호 노출, 아이디·비밀번호 평문 저장, 단일문자 사용에 따른 비밀번호 유출	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01 -09		본 제품(유헬스케어 게이트웨이)에서 로그인 시도 시, '암호가 올바르지 않습니다.' 등 이 문구를 표시하는 경우(이 경우 해당 ID 가 존재한다는 것을 알 수 있으므로 바람직하지 않음)를 이용한 특정 계정 탈취 시도	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-01 -10		본 제품(유헬스케어 게이트웨이)에 접근 시, SQL injection 등 인증 절차의 취약점을 통한 권한 획득 시도	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-02	비인가자의 불법 소프트웨어 설치나 실행으로 게이트웨이의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	환자 진료 시 기기 오작동으로 진료 수행 불가	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-03	전송 정보(제어, 의료정보)의 유출 및 위변조	스니핑을 통한 전송 정보의 유출 및 중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-04	게이트웨이에 저장된 정보의 위변조	중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-05	비인가자가 게이트웨이에 저장된 정보를 위변조하여 진단지원시스템으로 전송	비인가자가 게이트웨이를 탈취	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…
UH-06	게이트웨이에 저장 된 정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈	…	…

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
UH-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
UH-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
UH-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
UH-10	시스템 로그 부재	비인가자가 접속 기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 정보의 조회, 생성, 수정, 삭제 가능	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
UH-11	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
UH-12	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
UH-13	통신 서비스 거부, 통신 지연 등	네트워크 접속 가능한 의료기기에 지속적인 공격 트래픽을 전송하여 통신 단절 또는 지연 발생	환자 진료정보 전송 불가	진료 기회 박탈	...	...
...	...	...	...	...	...	...

※ 발생가능성 및 심각성은 위험관리계획서에 정의된 기준에 따라 평가한다.

6. 위험평가

※ 심각성 및 발생가능성 평가기준은 위험관리계획서에서 정의된 기준에 따라 기재한다.

6.1 심각성 평가기준

용어	단계	가능한 기술
치명적	5	심각한 상해, 사망
높음	4	신체기능의 영구적 장애 또는 신체 구조의 영구적 손상
중간	3	일시적이고 경미한 상해, 의학적 중재 필요
낮음	2	일시적인 불편, 의학적 중재 없이 가역적
무시	1	경미하고 단시간 불편

6.2 발생가능성 평가기준

용어	단계	정의 (p=판매건수를 척도로 한 발생건수)
상습적 발생 (Frequent)	6	1/10 ≦ P
자주 발생 (Probable)	5	1/50 ≦ P < 1/10
가끔 발생(Occasional)	4	1/200 ≦ P < 1/50
이따금 발생 (Remote)	3	1/350 ≦ P < 1/200
희박한 발생 (Improbable)	2	1/500 ≦ P < 1/350
발생가능 거의없는 (Incredible)	1	P<1/500

6.3 위험 허용 판정

상습적 발생	6	6	12	18	24	30
자주 발생	5	5	10	15	20	25
가끔 발생	4	4	8	12	16	20
이따금 발생	3	3	6	9	12	15
희박한 발생	2	2	4	6	8	10
발생가능 거의없는	1	1	2	3	4	5
		무시 1	낮음 2	중간 3	높음 4	치명적 5

- 수락(널리 허용 가능한 영역, Acceptable risk, Green Zone) Level 0~4
- 중간(합리적으로 실현할 수 있는 가장 낮은(ALARP) 영역, As Low As Reasonably Practicable, Yellow Zone) Level 5~11
- 비수락(허용할 수 없는 영역, Unacceptable risk, Red Zone) Level 12~30

6.4 위험평가

No.	위험분석(Risk analysis)						위험평가 (Risk evaluation)	
	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생가능성	심각성	위험	결과
UH-01-01	게이트웨이 정보에 비인가 접근으로 인한 환자 정보 조작	사용자 구분을 하지 않고 누구나 환자의 정보에 접근하도록 한 경우	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	3	2	6	중간
UH-01-02		하나의 계정에 여러 사용자가 동시에 접속한 경우, 데이터의 왜곡 발생	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-03		비인가자의 접속 시도를 감지하지 못하는 경우	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-04		보안이 취약한 공유기(Wi-Fi) 이용으로 사용자 접근 권한이 탈취된 경우	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-05		도난된 정상 사용자 계정으로 원격에서 서버에 접속	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-06		사용 유효기간이 경과(퇴사, 장기출장 등)한 사용자 계정으로 기기 접속	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-07		사용자가 자리를 비웠을 때 세션이 종료되지 않은 계정에 비인가자가 이용	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-08		로그인 시 비밀번호 노출, 아이디·비밀번호 평문 저장, 단일문자 사용에 따른 비밀번호 유출	조작 된 정보로 원격 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...

UH-01-09		본 제품(유헬스케어 게이트웨이)에서 로그인 시도 시, '암호가 올바르지 않습니다.' 등이 문구를 표시하는 경우(이 경우 해당 ID가 존재한다는 것을 알 수 있으므로 바람직하지 않음)를 이용한 특정 계정 탈취 시도	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-01-10		본 제품(유헬스케어 게이트웨이)에 접근 시, SQL injection 등 인증 절차의 취약점을 통한 권한 획득 시도	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-02	비인가자의 불법 소프트웨어 설치나 실행으로 게이트웨이의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	환자 진료 시 기기 오작동으로 진료 수행 불가	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-03	전송 정보(제어, 의료정보)의 유출 및 위변조	스니핑을 통한 전송 정보의 유출 및 중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-04	게이트웨이에 저장된 정보의 위변조	중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-05	비인가자가 게이트웨이에 저장된 정보를 위변조하여 진단지원시스템으로 전송	비인가자가 게이트웨이를 탈취	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...
UH-06	게이트웨이에 저장 된 정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈	...	...	...	...
UH-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...	...	...

UH-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…	…	…
UH-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…	…	…
UH-10	시스템 로그 부재	비인가자가 접속 기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 정보의 조회, 생성, 수정, 삭제 가능	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…	…	…
UH-11	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드 하여 기기 작동 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…	…	…
UH-12	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…	…	…
UH-13	통신 서비스 거부, 통신 지연 등	네트워크 접속 가능한 의료기기에 지속적인 공격 트래픽을 전송하여 통신 단절 또는 지연 발생	환자 진료정보 전송 불가	진료 기회 박탈	…	…	…	…
…	…	…	…	…	…	…	…	…

※ 위험관리계획서에 정의된 기준에 따라 발생가능성 및 심각성, 위험, 결과를 평가한다.

7. 위험통제

7.1 위험통제 조치

※ 위해요인의 ID(예: UH-01-01 등)에 RC를 추가하여 위험통제 조치의 항목을 식별한다.

No.	위험통제 조치 (Risk Control)	위험통제 조치 실행	잔여위험평가			결과	위험/이득분석	추가발생위험	통제완료
			발생가능성	심각성	위험				
UH-RC-01-01	설계 변경을 통한 사용자별 접근통제 및 인증 기능 구현	소프트웨어 검증 자료로 접근통제 및 인증 기능 구현 확인	**1**	**2**	**2**	**수락**	**N**	**N**	**Y**
UH-RC-01-02	설계 변경을 통한 동일 계정 다중접속 제한 기능 구현	소프트웨어 검증 자료로 다중접속 제한 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-01-03	설계 변경을 통한 비인가자의 접속 감지 및 제한 기능 구현	소프트웨어 검증 자료로 비인가자의 접속 감지 및 제한 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-01-04	설계 변경을 통한 네트워크를 통한 접속시 인증 기능 구현	소프트웨어 검증 자료로 네트워크를 통한 접속시 인증 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-01-05	설계 변경을 통한 분실 신고 계정에 대한 접속 제한 기능 구현	소프트웨어 검증 자료로 분실 신고 계정에 대한 접속 제한 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-01-06	설계 변경을 통한 사용자 계정 유효기간 설정 기능 구현	소프트웨어 검증 자료로 사용자 계정 유효기간 설정 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-01-07	설계 변경을 통한 세션 자동종료 기능 구현	소프트웨어 검증 자료로 세션 자동종료 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-01-08	설계 변경을 통한 비밀번호 작성 규칙 구현, 암호화, 마스킹, 피드백 미제공 구현	소프트웨어 검증 자료로 비밀번호 작성 규칙 구현, 암호화, 마스킹, 피드백 미제공 구현 확인	…	…	…	…	…	…	…
UH-RC-01-09	설계 변경을 통한 응답 메세지내 모호한 표현 사용 구현	소프트웨어 검증 자료로 응답 메세지내 모호한 표현 사용 구현 확인	…	…	…	…	…	…	…
UH-RC-01-10	설계 변경을 통한 입력 값 검증 코드 추가 및 우회 불가능한 사용자 인증 기능 구현	소프트웨어 검증 자료로 입력 값 검증 코드 추가 및 우회 불가능한 사용자 인증 기능 구현	…	…	…	…	…	…	…

UH-RC-02	설계 변경을 통한 필요한 서비스(포트, 권한 등)만 활성화	소프트웨어 검증 자료로 필요한 서비스(포트, 권한 등)만 활성화	…	…	…	…	…	…	…
UH-RC-03	설계 변경을 통한 전송 정보의 암호화 기능 구현	소프트웨어 검증 자료로 전송 정보의 암호화 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-04	설계 변경을 통한 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현	소프트웨어 검증 자료로 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-05	설계 변경을 통한 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현	소프트웨어 검증 자료로 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-06	설계 변경을 통한 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현	소프트웨어 검증 자료로 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-07	설계 변경을 통한 업데이트 시 인증 기능 구현	소프트웨어 검증 자료로 업데이트 시 인증 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-08	설계 변경을 통한 업데이트 시 무결성 체크 기능 구현	소프트웨어 검증 자료로 업데이트 시 무결성 체크 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-09	설계 변경을 통한 업데이트 제공자 인증 절차 기능 구현	소프트웨어 검증 자료로 업데이트 제공자 인증 절차 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-10	설계 변경을 통한 시스템 접속 및 정보 관리 로그 기능 구현	소프트웨어 검증 자료로 시스템 접속 및 정보 관리 로그 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-11	설계 변경을 통한 실행파일 실행전 무결성 체크 기능 구현	소프트웨어 검증 자료로 실행파일 실행전 무결성 체크 기능 구현 확인	…	…	…	…	…	…	…
UH-RC-12	설계 변경을 통한 보안 위협 탐지 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 보안 위협 탐지 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인	…	…	…	…	…	…	…

UH-RC-13	설계 변경을 통한 통신 오류 탐지 및 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 통신 오류 탐지 및 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…	…

※ 위험관리계획서에 정의된 기준에 따라 발생가능성 및 심각성, 위험, 결과, 위험/이득분석, 추가발생위험, 통제완료를 평가한다.

7.2 위험통제 조치 설명

No.	위험통제 조치(Risk Control)	위험통제 조치 설명
UH-RC-01-01	사용자별 접근통제 및 인증 기능	ID/PW로 사용자 구분 및 인증기능을 구현하고 각 계정별 접근할 수 있는 정보에 대한 권한을 차등적으로 부여한다.
UH-RC-01-02	동일 계정 다중접속 제한 기능	하나의 계정에 먼저 접속한 사용자가 있는 상태에서 동일 계정으로 추가 접속을 시도할 경우, 추가 접속을 시도한 사용자에게 접속 제한 관련 '동일 계정 다중접속을 제한합니다.' 와 같은 알림을 표시한다.
UH-RC-01-03	비인가자의 접속 감지 및 제한 기능	잘못 된 PW를 이용하여 지속적인 로그인 시도에 대해 감지하는 기능을 구현하고 PW를 5회이상 잘못 입력하면 해당 계정의 접속을 제한한다.
UH-RC-01-04	네트워크의 접속시 인증 기능	네트워크의 인증정보를 확인하여 접속한다.
UH-RC-01-05	분실 신고 계정에 대한 접속 제한 기능	사용자(의료기기)가 등록 된 단말기의 분실 신고 시 단말기의 인증정보를 제한한다.
UH-RC-01-06	사용자 계정 유효기간 설정 기능	사용자(의료기기) 계정의 유효기간은 1년으로 하고 만료 한달 전부터 갱신할 수 있도록 한다.
UH-RC-01-07	세션 자동종료 기능	접속 후 10분간 활동이 없으면 접속을 종료한다.
UH-RC-01-08	비밀번호 작성 규칙 구현, 암호화, 마스킹, 피드백 미제공	비밀번호는 숫자, 문자, 특수문자로 OO 자리 이상으로 하고 O 개월 마다 사용자에게 비밀번호 변경 안내를 제공한다. 비밀번호는 OO 프로토콜을 이용하여 암호화 한다. 비밀번호를 입력 시 ***로 표시한다.
UH-RC-01-09	응답 메세지내 모호한 표현 사용	'아이디가 없거나 비밀번호가 틀렸습니다'라는 응답 메시지를 제공한다.

UH-RC-01-10	입력 값 검증 코드 추가 및 우회 불가능한 사용자 인증 기능	ID/PW로 사용자 구분 및 인증기능을 구현한다.
UH-RC-02	필요한 서비스(포트, 권한 등)만 활성화	사용하는 서비스(포트, 권한 등)만 활성화 시킨다.
UH-RC-03	전송 정보의 암호화 기능	의료기기 제어정보, 개인의료정보 전송시 OO프로토콜을 이용하여 암호화한다.
UH-RC-04	게이트웨이에 의료정보를 저장하지 않고 송신하는 기능	진단지원시스템으로 전송 시 임시 저장 정보는 삭제한다.
UH-RC-05	게이트웨이에 의료정보를 저장하지 않고 송신하는 기능	진단지원시스템으로 전송 시 임시 저장 정보는 삭제한다.
UH-RC-06	게이트웨이에 의료정보를 저장하지 않고 송신하는 기능	진단지원시스템으로 전송 시 임시 저장 정보는 삭제한다.
UH-RC-07	업데이트 시 인증 기능	펌웨어 또는 소프트웨어 업데이트 시 관리자의 인가를 요청 및 확인하는 절차를 구현한다.
UH-RC-08	업데이트 시 무결성 체크 기능	펌웨어 또는 소프트웨어 업데이트 파일의 무결성을 체크하는 기능을 구현한다.
UH-RC-09	업데이트 제공자 인증 절차 기능	펌웨어 또는 소프트웨어 업데이트 시 디지털 서명 등의 방식으로 출처를 검증 후 진행한다.
UH-RC-10	시스템 접속 및 정보 관리 로그 기능	사용자의 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등 로그 정보를 기록한다.
UH-RC-11	실행파일 실행전 무결성 체크 기능	실행파일 및 설정파일에 대한 무결성을 체크하는 기능을 구현한다.
UH-RC-12	보안 위협 탐지 알람 기능 사용자매뉴얼을 통해 사용자에 대응 절차 제공	보안 위협에 따른 통신 오류, 지연 등, 기기 설정 변경, 비인가 접속 등을 탐지하여 사용자에게 알람을 제공한다. 이에 대한 제조자 담당자 연락처를 매뉴얼에 제공하고, 사이버 보안 위협 탐지 시 취해야 할 대응책 사용자에게 제공 한다.
UH-RC-13	통신 오류 탐지 및 알람 기능 사용자매뉴얼을 통해 사용자에 대응 절차 제공	통신 응답 신호의 시간을 모니터링하여 지정 시간이 초과하는 경우 사용자에게 통신 오류 알람을 제공한다. 이에 대한 제조자 담당자 연락처를 매뉴얼에 제공하고, 사이버 보안 위협 탐지 시 취해야 할 대응책 사용자에게 제공 한다.
		-
		-

8. 전체 잔여위험 허용가능성 평가

No.	잔여 위험평가			결과	위험/이득 분석	추가 발생 위험	통제 완료	전체 잔여위험 허용가능성 평가 (Evaluation of overall residual risk acceptability)
	발생 가능성	심각성	위험					허용가능 /허용불가
UH-RC-01-01	1	2	2	수락	N	N	Y	허용가능
UH-RC-01-02	…	…	…	…	…	…	…	…
UH-RC-01-03	…	…	…	…	…	…	…	…
UH-RC-01-04	…	…	…	…	…	…	…	…
UH-RC-01-05	…	…	…	…	…	…	…	…
UH-RC-01-06	…	…	…	…	…	…	…	…
UH-RC-01-07	…	…	…	…	…	…	…	…
UH-RC-01-08	…	…	…	…	…	…	…	…
UH-RC-01-09	…	…	…	…	…	…	…	…
UH-RC-01-10	…	…	…	…	…	…	…	…
UH-RC-02	…	…	…	…	…	…	…	…
UH-RC-03	…	…	…	…	…	…	…	…
UH-RC-04	…	…	…	…	…	…	…	…
UH-RC-05	…	…	…	…	…	…	…	…
UH-RC-06	…	…	…	…	…	…	…	…
UH-RC-07	…	…	…	…	…	…	…	…

UH-RC-08	…	…	…	…	…	…	…	…
UH-RC-09	…	…	…	…	…	…	…	…
UH-RC-10	…	…	…	…	…	…	…	…
UH-RC-11	…	…	…	…	…	…	…	…
UH-RC-12	…	…	…	…	…	…	…	…
UH-RC-13	…	…	…	…	…	…	…	…
…								

9. 위험관리보고서

※ 위험관리보고서는 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

10. 생산 및 생산 후 정보 입수를 위한 방법

※ 생산 및 생산 후 정보 입수를 위한 방법은 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

11. FMEA 보고서

No.	위험분석 (Risk analysis)						위험 평가 (Risk evaluation)		위험통제 (Risk control)								전체 잔여 위험 허용 가능성 평가
	위해 요인	발생 가능한 사례	위해상황	위해	발생가능성	심각성	위험	결과	위험 통제 조치	위험통제조치 실행	발생가능성	심각성	위험	결과	위험이득분석	추가발생위험	통제완료	허용 가능 / 허용 불가
UH-01-01	게이트웨이 정보에 비인가 접근으로 인한 환자 정보 조작	사용자 구분을 하지 않고 누구나 환자의 정보에 접근하도록 한 경우	조작된 정보로 원격진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	3	2	6	중간	설계 변경을 통한 사용자별 접근통제 및 인증 기능 구현	소프트웨어 검증 자료로 접근통제 및 인증 기능 구현 확인	1	2	2	수락	N	N	Y	허용 가능
UH-01-02		하나의 계정에 여러 사용자가 동시에 접속한 경우, 데이터의 왜곡 발생	조작된 정보로 원격진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 동일계정 다중접속 제한 기능 구현	소프트웨어 검증 자료로 다중접속 제한 기능 구현 확인	…	…	…	…	…	…	…	
UH-01-03		비인가자의 접속 시도를 감지하지 못하는 경우	조작된 정보로 원격진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 비인가자의 접속 감지 및 제한 기능 구현	소프트웨어 검증 자료로 비인가자의 접속 감지 및 제한 기능 구현 확인	…	…	…	…	…	…	…	
UH-01-04		보안이 취약한 공유기(Wi-Fi) 이용으로 사용자 접근 권한이 탈취된 경우	조작된 정보로 원격진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 네트워크를 통한 접속시 인증 기능 구현	소프트웨어 검증 자료로 네트워크를 통한 접속시 인증 기능 구현 확인								

UH-01-05		도난된 정상 사용자 계정으로 원격에서 서버에 접속	조작된 정보로 원격 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 분실 신고 계정에 대한 접속 제한 기능 구현	소프트웨어 검증 자료로 분실 신고 계정에 대한 접속 제한 기능 구현 확인								
UH-01-06		사용 유효기간이 경과(퇴사, 장기출장 등)한 사용자 계정으로 기기 접속	조작된 정보로 원격 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 사용자 계정 유효기간 설정 기능 구현	소프트웨어 검증 자료로 사용자 계정 유효기간 설정 기능 구현 확인								
UH-01-07		사용자가 자리를 비웠을 때 세션이 종료되지 않은 계정에 비인가자가 이용	조작된 정보로 원격 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 세션 자동종료 기능 구현	소프트웨어 검증 자료로 세션 자동종료 기능 구현 확인								
UH-01-08		로그인 시 비밀번호 노출, 아이디·비밀번호 평문 저장, 단일문자 사용에 따른 비밀번호 유출	조작된 정보로 원격 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 비밀번호 작성 규칙 구현, 암호화, 마스킹, 피드백 미제공 구현	소프트웨어 검증 자료로 비밀번호 작성 규칙 구현, 암호화, 마스킹, 피드백 미제공 구현 확인								
UH-01-09		본 제품(유헬스케어 게이트웨이)에서 로그인 시도 시, '암호가 올바르지 않습니다.' 등이 문구를 표시하는 경우(이 경우 해당 ID 가 존재한다는 것을 알 수 있으므로 바람직하지 않음)를 이용한 특정 계정 탈취 시도	조작된 정보로 원격 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 응답 메세지내 모호한 표현 사용 구현	소프트웨어 검증 자료로 응답 메세지내 모호한 표현 사용 구현 확인								
UH-01-10		본 제품(유헬스케어 게이트웨이)에 접근 시, SQL injection 등 인증 절차의 취약점을 통한 권한 획득 시도	조작된 정보로 원격 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 입력 값 검증 코드 추가 및 우회 불가능한 사용자 인증 기능 구현	소프트웨어 검증 자료로 입력 값 검증 코드 추가 및 우회 불가능한 사용자 인증 기능 구현								

UH-02	비인가자의 불법 소프트웨어 설치나 실행으로 게이트웨이의 오작동	외부 네트워크로부터 기기에서 활성화된 통신 서비스를 통해 접속	환자 진료 시 기기 오작동으로 진료 수행 불가	오진 잘못된 치료 수행 또는 치료 기회 박탈	...	...	...	...	설계 변경을 통한 필요한 서비스(포트, 권한 등)만 활성화	소프트웨어 검증 자료로 필요한 서비스(포트, 권한 등)만 활성화 확인								
UH-03	전송 정보(제어, 의료정보)의 유출 및 위변조	스니핑을 통한 전송 정보의 유출 및 중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	...	...	...	...	설계 변경을 통한 전송 정보의 암호화 기능 구현	소프트웨어 검증 자료로 전송 정보의 암호화 기능 구현 확인								
UH-04	게이트웨이에 저장된 정보의 위변조	중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	...	...	...	...	설계 변경을 통한 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현	소프트웨어 검증 자료로 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현 확인								
UH-05	비인가자가 게이트웨이에 저장된 정보를 위변조하여 진단지원시스템으로 전송	비인가자가 게이트웨이를 탈취	조작 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	...	...	...	...	설계 변경을 통한 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현	소프트웨어 검증 자료로 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현 확인								
UH-06	게이트웨이에 저장 된 정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치 료 기 회 박탈	...	...	...	...	설계 변경을 통한 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현	소프트웨어 검증 자료로 게이트웨이에 의료정보를 저장하지 않고 송신하는 기능 구현 확인								
UH-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	...	...	...	...	설계 변경을 통한 업데이트 시 인증 기능 구현	소프트웨어 검증 자료로 업데이트 시 인증 기능 구현 확인								

UH-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 업데이트 시 무결성 체크 기능 구현	소프트웨어 검증 자료로 업데이트 시 무결성 체크 기능 구현 확인								
UH-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 업데이트 제공자 인증 절차 기능 구현	소프트웨어 검증 자료로 업데이트 제공자 인증 절차 기능 구현 확인								
UH-10	시스템 로그 부재	비인가자가 접속기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 정보의 조회, 생성, 수정, 삭제 가능	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 시스템 접속 및 정보 관리 로그 기능 구현	소프트웨어 검증 자료로 시스템 접속 및 정보 관리 로그 기능 구현 확인								
UH-11	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 실행파일 실행전 무결성 체크 기능 구현	소프트웨어 검증 자료로 실행파일 실행전 무결성 체크 기능 구현 확인								

UH-12	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	환자 진료 시 기기 오작동으로 진료 수행 불가 및 위변조 된 정보로 진료 수행	오진 잘못된 치료 수행 또는 치료 기회 박탈	…	…	…	…	설계 변경을 통한 보안 위협 탐지 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 보안 위협 탐지 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인								
UH-13	통신 서비스 거부, 통신 지연 등	네트워크 접속 가능한 의료기기에 지속적인 공격 트래픽을 전송하여 통신 단절 또는 지연 발생	환자 진료 정보 전송 불가	진료 기회 박탈	…	…	…	…	설계 변경을 통한 통신 오류 탐지 및 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 통신 오류 탐지 및 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인								
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

나. 범용초음파영상진단장치

1. 개요 및 소개

※ 개요 및 소개는 본 예시에서 생략한다.

2. 용어 정의

※ 용어 정의는 본 예시에서 생략한다.(2등급 유헬스케어 게이트웨이 참조)

3. 제품 설명

※ 모양 및 구조, 원재료, 제조방법, 사용방법, 사용 시 주의사항, 포장단위, 저장방법 및 사용기간, 시험규격 등 일반적인 제품의 사항은 본 예시에서 생략한다.

3.1 제품명

. **품 목 명** : 범용초음파영상진단장치
. **품목분류번호** : A26380.01
. **등 급** : 2등급
. **모 델 명** : MFDS2

3.2 사용목적 : 진단을 위하여 환부에 초음파 에너지를 전송, 반사 신호를 수신하여 영상화하는 일반적인 초음파 영상 진단장치. 초음파 정보의 수집, 표시 및 분석에 사용하는 다양한 트랜스듀서 및 관련 어플리케이션 소프트웨어 패키지를 지원하고 있다.

3.3 사용환경 : 의료기관

3.4 소프트웨어 운영환경

- 내장형 소프트웨어, Window 7 이상

<범용초음파영상진단장치[2] 통신 구성도>

3.4 통신목적

- 제조원 서버와 범용초음파영상진단장치[2] : 소프트웨어 업데이트 등 유지보수
- 범용초음파영상진단장치[2]와 의료영상전송장치소프트웨어[2] : 의료영상, 환자식별정보 등 진료정보 송신

3.5 통신시나리오

- 의료기관 내 인가된 사용자가 본 제품을 이용하여 실시간으로 환자를 진단하여 그 결과 영상을 기록하거나 타과 또는 추가 외래 방문 시 활용을 위해 유선 통신을 이용하여 의료영상전송장치로 영상을 전송
- 내장되어 있는 펌웨어를 통해 통신 기능 수행

3.6 통신사양

- 제조원 서버와 범용초음파영상진단장치[2] 간 통신 : 유선 LAN 통신
- 범용초음파영상진단장치[2]와 의료영상전송장치소프트웨어[2] 간 통신 : 유선 LAN 통신

3.7 보안특성

- SSL 암호화

4. 위험분석 흐름도

※ 위험분석 흐름도는 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

5. 위험분석

5.1 위해요인의 식별

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
US-01	비인가 접근	범용초음파영상진단장치 설정 메뉴에 비인가 접근으로 인한 환자 정보 조작	상해, 오진	미 FDA Recall/ 체크리스트 1.1/1.3/1.4/1.5/ 1.7/1.8/1.9
US-02		비인가자의 불법 소프트웨어 설치나 실행으로 범용초음파영상진단장치의 오작동	상해, 오진	미 FDA Recall/ 체크리스트 1.19
US-03	정보 위변조	범용초음파영상진단장치에서 의료영상전송장치로 전송 시 위변조	상해, 오진	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트1.15/ 1.16/1.17
US-04		범용초음파영상진단장치에 저장된 영상 정보의 위변조	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트 1.17/1.20
US-05		정보가 알 수 없는 방법으로 암호화 된 경우	치료기회 박탈	미 FDA Recall
US-06		장치의 설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	상해, 오진	미 FDA Recall
US-07	플래폼 또는 하드웨어 취약	무허가 업데이트	상해, 오진	의료기기 이상사례보고 / 체크리스트 1.12
US-08		무결성이 보장되지 않은 업데이트	상해, 오진	의료기기 이상사례보고 / 체크리스트 1.13
US-09		인증되지 않은 업데이트	상해, 오진	의료기기 이상사례보고 / 체크리스트 1.14
US-10		물리적 통신포트 제공	상해, 오진	의료기기 이상사례보고 / 체크리스트 1.18

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
US-11		시스템 로그 부재	상해, 오진	의료기기 이상사례보고 / 체크리스트 2.1
US-12		무결성이 보장되지 않은 실행파일 및 설정파일	상해, 오진	의료기기 이상사례보고 / 체크리스트 2.2
US-13		사이버 보안 위협 탐지 시 대응책 부재	상해, 오진	의료기기 이상사례보고 / 체크리스트 2.3
US-14				
US-15				
US-16				
...	...	...	...	...

※ 관련 자료 중 미 FDA Recall은 해당 제품 또는 유사 제품의 국외 Recall 사례를 의미함

5.2 각 위해 상황에서의 위험 산정

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
US-01-01	범용초음파영상진단장치 설정 메뉴에 비인가 접근으로 인한 환자 정보 조작	접근통제 기능 없이 누구나 범용초음파영상장치 설정에 접근하도록 한 경우	초음파 출력 조작, 설정 조작	상해, 오진	...	...
US-01-02		비인가자의 설정메뉴 접근 시도를 감지하지 못하는 경우	초음파 출력 조작, 설정 조작	상해, 오진	...	...
US-01-03		보안이 취약한 공유기 이용으로 사용자 접근 권한이 탈취된 경우	초음파 출력 조작, 설정 조작	상해, 오진	...	...
US-01-04		사용 유효기간이 경과(의료기관 조작자 또는 기업 유지보수 관리자 퇴사, 장기출장 등)한 사용자 계정으로 기기 접속	초음파 출력 조작, 설정 조작	상해, 오진	...	...

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
US-01-05		관리자가 설정 완료 후 설정 메뉴 접근을 종료하지 않고 자리를 비웠을 때 비인가자가 이용	초음파 출력 조작, 설정 조작	상해, 오진	...	...
US-01-06		설정 메뉴 접근 권한을 가진 사용자 변경 시 이전 사용자가 비밀번호를 알아 불법 접근	초음파 출력 조작, 설정 조작	상해, 오진	...	...
US-02	비인가자의 불법 소프트웨어 설치나 실행으로 범용초음파영상진단장치의 오작동	외부 네트워크로부터 기기에서 활성화된 통신 서비스를 통해 접속	초음파 출력 조작, 설정 조작	상해, 오진	...	...
US-03	범용초음파영상진단장치에서 의료영상전송장치로 전송 시 위변조	스니핑 등 중간자 공격	조작 된 영상으로 진료	상해, 오진	...	...
US-04	범용초음파영상진단장치에 저장된 영상 정보의 위변조	해킹에 의한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	...	...
US-05	정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈		
US-06	장치의 설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	중간자공격으로 인해 장치의 초음파 출력 설정을 조작	초음파 출력 조작, 설정 조작	상해, 오진		
US-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	초음파 출력 조작, 설정 조작	상해, 오진		
US-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	초음파 출력 조작, 설정 조작	상해, 오진		
US-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	초음파 출력 조작, 설정 조작	상해, 오진		

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
US-10	물리적 통신포트 제공	기기에 설치된 디버깅(개발자용) 포트로 기기 접속	초음파 출력 조작, 설정 조작	상해, 오진		
US-11	시스템 로그 부재	비인가자가 접속기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 기기 설정 변경	초음파 출력 조작, 설정 조작	상해, 오진		
US-12	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	초음파 출력 조작, 설정 조작	상해, 오진		
US-13	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	초음파 출력 조작, 설정 조작	상해, 오진		
…	…	…	…	…	…	…

※ 발생가능성 및 심각성은 위험관리계획서에 정의된 기준에 따라 평가한다.

6. 위험평가

※ 심각성 및 발생가능성 평가기준은 위험관리계획서에서 정의된 기준에 따라 기재한다.

6.1 심각성 평가기준

용어	단계	가능한 기술
치명적	5	심각한 상해, 사망
높음	4	신체기능의 영구적 장애 또는 신체 구조의 영구적 손상
중간	3	일시적이고 경미한 상해, 의학적 중재 필요
낮음	2	일시적인 불편, 의학적 중재 없이 가역적
무시	1	경미하고 단시간 불편

6.2 발생가능성 평가기준

용어	단계	정의 (p=판매건수를 척도로 한 발생건수)
상습적 발생 (Frequent)	6	1/10 ≦ P
자주 발생 (Probable)	5	1/50 ≦ P < 1/10
가끔 발생(Occasional)	4	1/200 ≦ P < 1/50
이따금 발생 (Remote)	3	1/350 ≦ P < 1/200
희박한 발생 (Improbable)	2	1/500 ≦ P < 1/350
발생가능 거의없는 (Incredible)	1	P<1/500

6.3 위험 허용 판정

상습적 발생	6	6	12	18	24	30
자주 발생	5	5	10	15	20	25
가끔 발생	4	4	8	12	16	20
이따금 발생	3	3	6	9	12	15
희박한 발생	2	2	4	6	8	10
발생가능 거의없는	1	1	2	3	4	5
		무시 1	낮음 2	중간 3	높음 4	치명적 5

- 수락(널리 허용 가능한 영역, Acceptable risk, Green Zone) Level 0~4
- 중간(합리적으로 실현할 수 있는 가장 낮은(ALARP) 영역, As Low As Reasonably Practicable, Yellow Zone) Level 5~11
- 비수락(허용할 수 없는 영역, Unacceptable risk, Red Zone) Level 12~30

6.4 위험평가

No.	위험분석(Risk analysis)						위험평가 (Risk evaluation)	
	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성	위험	결과
US-01-01	범용초음파영상진단장치 설정 메뉴에 비인가 접근으로 인한 환자 정보	접근통제 기능 없이 누구나 범용초음파영상장치 설정에 접근하도록 한 경우	초음파 출력 조작, 설정 조작	상해, 오진	3	2	6	중간

US-01-02	조작	비인가자의 설정메뉴 접근 시도를 감지하지 못하는 경우	초음파 출력 조작, 설정 조작	상해, 오진	...	...	...	...
US-01-03		보안이 취약한 공유기 이용으로 사용자 접근 권한이 탈취된 경우	초음파 출력 조작, 설정 조작	상해, 오진	...	...	...	...
US-01-04		사용 유효기간이 경과(의료기관 조작자 또는 기업 유지보수 관리자 퇴사, 장기출장 등)한 사용자 계정으로 기기 접속	초음파 출력 조작, 설정 조작	상해, 오진	...	...	...	...
US-01-05		관리자가 설정 완료 후 설정 메뉴 접근을 종료하지 않고 자리를 비웠을 때 비인가자가 이용	초음파 출력 조작, 설정 조작	상해, 오진	...	...	...	...
US-01-06		설정 메뉴 접근 권한을 가진 사용자 변경 시 이전 사용자가 비밀번호를 알아 불법 접근	초음파 출력 조작, 설정 조작	상해, 오진	...	...	...	...
US-02	비인가자의 불법 소프트웨어 설치나 실행으로 범용초음파영상진단장치의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	초음파 출력 조작, 설정 조작	상해, 오진	...	...	...	...
US-03	범용초음파영상진단장치에서 의료영상전송장치로 전송시 위변조	스니핑 등 중간자 공격	조작 된 영상으로 진료	상해, 오진	...	...	...	...

US-04	범용초음파영상진단장치에 저장된 영상 정보의 위변조	해킹에 의한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	…	…	…	…
US-05	정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈	…	…	…	…
US-06	장치의 설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	중간자공격으로 인해 장치의 초음파 출력 설정을 조작	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
US-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
US-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
US-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
US-10	물리적 통신포트 제공	기기에 설치된 디버깅(개발자용) 포트로 기기 접속	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
US-11	시스템 로그 부재	비인가자가 접속기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 기기 설정 변경	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
US-12	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…

US-13	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	초음파 출력 조작, 설정 조작	상해, 오진	…	…	…	…
…	…	…	…	…	…	…	…	…

※ 위험관리계획서에 정의된 기준에 따라 발생가능성 및 심각성, 위험, 결과를 평가한다.

7. 위험통제

7.1 위험통제 조치

No.	위험통제 조치 (Risk Control)	위험통제 조치 실행	잔여위험평가			결과	위험/이득분석	추가발생위험	통제완료
			발생가능성	심각성	위험				
US-RC-01-01	설계 변경을 통한 설정메뉴 접근통제 및 인증 기능 구현	소프트웨어 검증 자료로 접근통제 및 인증 기능 구현 확인	1	2	2	수락	N	N	Y
US-RC-01-02	설계 변경을 통한 비인가자의 접근 감지 및 제한 기능 구현	소프트웨어 검증 자료로 비인가자의 접근 감지 및 제한 기능 구현 확인							
US-RC-01-03	설계 변경을 통한 네트워크를 통한 접속 시 인증 기능 구현	소프트웨어 검증 자료로 네트워크를 통한 접속 시 인증 기능 구현 확인							
US-RC-01-04	설계 변경을 통한 관리자 계정 유효기간 설정 기능 구현	소프트웨어 검증 자료로 관리자 계정 유효기간 설정 기능 구현 확인							
US-RC-01-05	설계 변경을 통한 설정 메뉴 세션 자동종료 기능 구현	소프트웨어 검증 자료로 세션 자동 종료 기능 구현 확인							
US-RC-01-06	설계 변경을 통한 주기적 비밀번호 변경 기능 구현 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공	소프트웨어 검증 자료로 주기적 비밀번호 변경 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공 확인							

US-RC-02	설계 변경을 통한 불필요한 서비스 비활성화	소프트웨어 검증 자료로 불필요한 서비스 비활성화 확인							
US-RC-03	설계 변경을 통한 전송 정보의 암호화 기능 구현	소프트웨어 검증 자료로 전송 정보의 암호화 기능 구현 확인							
US-RC-04	해시값 비교를 통한 정보의 무결성 확인 ※ 다른 통제조치로 암호화나 기기 내 영상을 저장하지 않는 방식으로 구현할 수 있다.	저장된 데이터의 해시값을 비교하여 데이터 변조사항 확인 및 복구							
US-RC-05	설계 변경을 통한 유효하지 않은 영상 데이터에 대한 사용 중단 및 사용자 알림 기능 구현 ※ 전송 시, 기기 내 영상을 저장하지 않는 방식으로 구현할 수 있다.	소프트웨어 검증 자료로 유효하지 않은 영상 데이터에 대한 사용 중단 및 사용자 알림 기능 구현 확인							
US-RC-06	설계 변경을 통한 원격 설정 기능 차단 기능 구현	소프트웨어 검증 자료로 원격 설정 기능 차단 구현 확인							
US-RC-07	설계 변경을 통한 업데이트 시 인증 기능 구현	소프트웨어 검증 자료로 업데이트 시 인증 기능 구현 확인							
US-RC-08	설계 변경을 통한 업데이트 시 무결성 체크 기능 구현	소프트웨어 검증 자료로 업데이트 시 무결성 체크 기능 구현 확인							
US-RC-09	설계 변경을 통한 업데이트 제공자 인증 절차 기능 구현	소프트웨어 검증 자료로 업데이트 제공자 인증 절차 기능 구현 확인							
US-RC-10	물리적 통신포트 잠금 혹은 제거	물리적 통신포트 제공여부 확인							
US-RC-11	설계 변경을 통한 시스템 접속 및 정보 관리 로그 기능 구현	소프트웨어 검증 자료로 시스템 접속 및 정보 관리 로그 기능 구현 확인							

US-RC-12	설계 변경을 통한 실행파일 실행전 무결성 체크 기능 구현	소프트웨어 검증 자료로 실행파일 실행전 무결성 체크 기능 구현 확인							
US-RC-13	설계 변경을 통한 보안 위협 탐지 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 보안 위협 탐지 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인							
...	...	...	...	...	...	...	...	...	...

※ 위험관리계획서에 정의된 기준에 따라 발생가능성 및 심각성, 위험, 결과, 위험/이득분석, 추가발생위험, 통제완료를 평가한다.

7.2 위험통제 조치 설명

No.	위험통제 조치(Risk Control)	위험통제 조치 설명
US-RC-01-01	설정메뉴 접근통제 및 인증 기능	설정 메뉴 접근 시 인증번호를 입력하도록 구현한다.
US-RC-01-02	비인가자의 접근 감지 및 제한 기능	잘못 된 PW를 이용하여 지속적인 로그인 시도에 대해 감지하는 기능을 구현하고 PW를 5회이상 잘못 입력하면 해당 메뉴의 접속을 제한한다.
US-RC-01-03	네트워크를 통한 접속시 인증 기능	네트워크의 인증정보를 확인하여 접속한다.
US-RC-01-04	관리자 계정 유효기간 설정 기능	PW는 3개월 주기로 변경을 알리는 메세지를 제공한다.
US-RC-01-05	설정 메뉴 세션 자동종료 기능	접속 후 10분간 활동이 없으면 접속을 종료한다.
US-RC-01-06	주기적 비밀번호 변경 기능 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공	PW는 3개월 주기로 변경을 알리는 메세지를 제공하고 관리 상 주의사항을 제공한다.
US-RC-02	불필요한 서비스 비활성화	불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 유지보수를 위한 포트는 IP를 제한하여 접속한다.
US-RC-03	전송 정보의 암호화 기능	의료영상, 개인의료정보 전송시 OO프로토콜을 이용하여 암호화한다.
US-RC-04	해시값 비교를 통한 정보의 무결성 확인	저장된 데이터의 해시값을 비교하여 데이터의 변조사항을 확인하고 데이터가 변조된 경우 정상 복구한다.

US-RC-05	영상 데이터 감영 여부 체크 기능 및 알람 기능	영상 데이터 감영 여부를 체크하고 감염 등 정상 데이터가 아닌 경우 사용자에게 시각 또는 청각적으로 경고한다.
US-RC-06	원격 설정 기능 차단 기능	기기 설정 메뉴는 오프라인으로만 접근하도록 한다.
US-RC-07	업데이트 시 인증 기능	펌웨어 또는 소프트웨어 업데이트 시 관리자의 인가를 요청 및 확인하는 절차를 구현한다.
US-RC-08	업데이트 시 무결성 체크 기능	펌웨어 또는 소프트웨어 업데이트 파일의 무결성을 체크하는 기능을 구현한다.
US-RC-09	업데이트 제공자 인증 절차 기능	펌웨어 또는 소프트웨어의 업데이트 시 인증된 코드로 제한 한다.
US-RC-10	물리적 통신포트 잠금 혹은 제거	펌웨어 업데이트를 위한 포트는 출고 시 비활성화 한다.
US-RC-11	시스템 접속 및 정보 관리 로그 기능	사용자의 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등 로그 정보를 기록한다.
US-RC-12	실행파일 실행전 무결성 체크 기능	실행파일 및 설정파일에 대한 무결성을 체크하는 기능을 구현한다.
US-RC-13	보안 위협 탐지 알람 기능 사용자매뉴얼을 통해 사용자에 대응 절차 제공	보안 위협에 따른 통신 오류, 지연 등, 기기 설정 변경, 비인가 접속 등을 탐지하여 사용자에게 알람을 제공한다. 이에 대한 제조자 담당자 연락처를 매뉴얼에 제공하고, 사이버 보안 위협 탐지 시 취해야 할 대응책 사용자에게 제공 한다.
		-
		-

8. 전체 잔여위험 허용가능성 평가

No.	잔여 위험평가			결과	위험/이득 분석	추가 발생 위험	통제 완료	전체 잔여위험 허용가능성 평가 (Evaluation of overall residual risk acceptability)
	발생 가능성	심각성	위험					허용가능 /허용불가
US-RC-01-01	1	2	2	수락	N	N	Y	허용가능
US-RC-01-02	…	…	…	…	…	…	…	…
US-RC-01-03	…	…	…	…	…	…	…	…
US-RC-01-04	…	…	…	…	…	…	…	…
US-RC-01-05	…	…	…	…	…	…	…	…
US-RC-01-06	…	…	…	…	…	…	…	…
US-RC-02	…	…	…	…	…	…	…	…
US-RC-03	…	…	…	…	…	…	…	…
US-RC-04	…	…	…	…	…	…	…	…
US-RC-05	…	…	…	…	…	…	…	…
US-RC-06	…	…	…	…	…	…	…	…
US-RC-07	…	…	…	…	…	…	…	…
US-RC-08	…	…	…	…	…	…	…	…
US-RC-09	…	…	…	…	…	…	…	…
US-RC-10	…	…	…	…	…	…	…	…
US-RC-11	…	…	…	…	…	…	…	…
US-RC-12	…	…	…	…	…	…	…	…

US-RC-13	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…
…								

9. 위험관리보고서

※ 위험관리보고서는 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

10. 생산 및 생산 후 정보 입수를 위한 방법

※ 생산 및 생산 후 정보 입수를 위한 방법은 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

11. FMEA 보고서

No.	위험분석 (Risk analysis)						위험 평가 (Risk evaluation)		위험통제 (Risk control)								전체 잔여 위험 허용 가능성 평가
	위해 요인	발생 가능한 사례	위해상황	위해	발생가능성	심각성	위험	결과	위험 통제 조치	위험통제조치 실행	발생가능성	심각성	위험	결과	위험이득분석	추가발생위험	통제완료	허용 가능 / 허용 불가
US-01-01	범용초음파영상진단장치 설정 메뉴에 비인가 접근으로 인한 환자 정보 조작	접근통제 기능 없이 누구나 범용초음파 영상장치 설정에 접근하도록 한 경우	초음파 출력 조작, 설정 조작	상해, 오진	3	2	6	중간	설계 변경을 통한 설정메뉴 접근 통제 및 인증 기능 구현	소프트웨어 검증 자료로 접근통제 및 인증 기능 구현 확인	1	2	2	수락	N	N	Y	허용 가능
US-01-02		비인가자의 설정메뉴 접근 시도를 감지하지 못하는 경우	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 비인가자의 접근 감지 및 제한 기능 구현	소프트웨어 검증 자료로 비인가자의 접근 감지 및 제한 기능 구현 확인								
US-01-03		보안이 취약한 공유기 이용으로 사용자 접근 권한이 탈취된 경우	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 네트워크를 통한 접속시 인증 기능 구현	소프트웨어 검증 자료로 네트워크를 통한 접속시 인증 기능 구현 확인								
US-01-04		사용 유효기간이 경과(의료기관 조작자 또는 기업 유지보수 관리자 퇴사, 장기출장 등)한 사용자 계정으로 기기 접속	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 관리자 계정 유효기간 설정 기능 구현	소프트웨어 검증 자료로 관리자 계정 유효기간 설정 기능 구현 확인								
US-01-05		관리자가 설정 완료 후 설정 메뉴 접근을 종료하지 않고 자리를 비웠을 때 비인가자가 이용	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 설정 메뉴 세션 자동종료 기능 구현	소프트웨어 검증 자료로 세션 자동종료 기능 구현 확인								

US-01-06		설정 메뉴 접근 권한을 가진 사용자 변경 시 이전 사용자가 비밀번호를 알아 불법 접근	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 주기적 비밀번호 변경 기능 구현 및 사용자 매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공	소프트웨어 검증 자료로 주기적 비밀번호 변경 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공 확인								
US-02	비인가자의 불법 소프트웨어 설치나 실행으로 범용초음파영상진단장치의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 불필요한 서비스 비활성화	소프트웨어 검증 자료로 불필요한 서비스 비활성화 확인								
US-03	범용초음파영상진단장치에서 의료영상전송장치로 전송 시 위변조	스니핑 등 중간자 공격	조작 된 영상으로 진료	상해, 오진					설계 변경을 통한 전송 정보의 암호화 기능 구현	소프트웨어 검증 자료로 전송 정보의 암호화 기능 구현 확인								
US-04	범용초음파영상진단장치에 저장된 영상 정보의 위변조	해킹에 의한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈					해시값 비교를 통한 정보의 무결성 확인	저장된 데이터의 해시값을 비교하여 데이터의 변조사항을 확인하고 데이터가 변조된 경우 정상 복구								
US-05	정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈					설계 변경을 통한 유효하지 않은 영상 데이터에 대한 사용 중단 및 사용자 알림 기능 구현	소프트웨어 검증 자료로 유효하지 않은 영상 데이터에 대한 사용 중단 및 사용자 알림 기능 구현 확인								
US-06	장치의 설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	중간자공격으로 인해 장치의 초음파 출력 설정을 조작	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 원격 설정 기능 차단 기능 구현	소프트웨어 검증 자료로 원격 설정 기능 차단 구현 확인								
US-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨	초음파 출력 조작,	상해, 오진					설계 변경을 통한 업데이트 시	소프트웨어 검증 자료로 업데이트								

		어 업데이트 시도	설정 조작						인증 기능 구현	시 인증 기능 구현 확인									
US-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 업데이트 시 무결성 체크 기능 구현	소프트웨어 검증 자료로 업데이트 시 무결성 체크 기능 구현 확인									
US-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 업데이트 제공자 인증 절차 기능 구현	소프트웨어 검증 자료로 업데이트 제공자 인증 절차 기능 구현 확인									
US-10	물리적 통신포트 제공	기기에 설치된 디버깅(개발자용) 포트로 기기 접속	초음파 출력 조작, 설정 조작	상해, 오진					물리적 통신포트 잠금 혹은 제거	물리적 통신포트 제공여부 확인									
US-11	시스템 로그 부재	비인가자가 접속기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 기기 설정 변경	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 시스템 접속 및 정보 관리 로그 기능 구현	소프트웨어 검증 자료로 시스템 접속 및 정보 관리 로그 기능 구현 확인									
US-12	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 실행파일 실행전 무결성 체크 기능 구현	소프트웨어 검증 자료로 실행파일 실행전 무결성 체크 기능 구현 확인									
US-13	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안 사고 발생 유도	초음파 출력 조작, 설정 조작	상해, 오진					설계 변경을 통한 보안 위협 탐지 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 보안 위협 탐지 알람 기능 구현 확인 및 사용자 매뉴얼을 통해 사용자에 대응 절차 제공 확인									

...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

다. 환자감시장치

1. 개요 및 소개

※ 개요 및 소개는 본 예시에서 생략한다.

2. 용어 정의

※ 용어 정의는 본 예시에서 생략한다.(2등급 유헬스케어 게이트웨이 참조)

3. 제품 설명

※ 모양 및 구조, 원재료, 제조방법, 사용방법, 사용 시 주의사항, 포장단위, 저장방법 및 사용기간, 시험규격 등 일반적인 제품의 사항은 본 예시에서 생략한다.

3.1 제품명

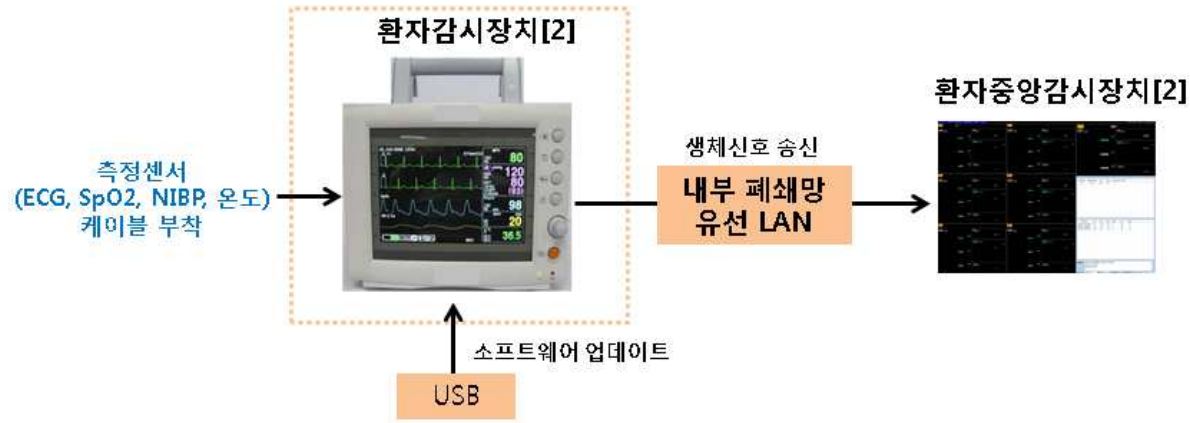
. **품 목 명** : 환자감시장치
. **품목분류번호** : A26090.01
. **등 급** : 2등급
. **모 델 명** : MFDS3

3.2 사용목적 : 환자의 각종 생체 정보 현상을 감시하는 기구로서 유해한 경우에는 시각 또는 청각 등에 의한 경보를 발생한다.

3.3 사용환경 : 의료기관

3.4 소프트웨어 운영환경

- 내장형 소프트웨어, Window XP 이상



<환자감시장치[2] 통신 구성도>

3.4 통신목적

- 환자감시장치[2]와 USB 통신 : 소프트웨어 업데이트 등 유지보수
- 환자감시장치[2]와 환자중앙감시장치[2] : 생체신호(심전도, 산소포화도, 체온), 환자식별 정보 등 진료정보 송신

3.5 통신시나리오

- 내장되어 있는 펌웨어를 통해 환자감시장치에서 실시간으로 감시하는 생체정보, 알람 등을 간호사실 등에서도 추가로 감시하기 위해 환자중앙감시장치로 송신
- 생체정보 및 알람 정보는 본 제품에 임시저장하나 환자중앙감시장치로 전송 시 삭제

3.6 통신사양

- 환자감시장치[2] 유지보수 : USB 통신
- 환자감시장치[2]와 환자중앙감시장치[2] 간 통신 : 유선 LAN 통신

3.7 보안특성

- 환자감시장치[2]와 환자중앙감시장치[2] 간 통신 : SSL 암호화

4. 위험분석 흐름도

※ 위험분석 흐름도는 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

5. 위험분석

5.1 위해요인의 식별

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
PM-01	비인가 접근	환자감시장치의 알람 등 설정 메뉴에 비인가 접근으로 기기 설정 조작	환자 위험 상황 시 알람 미작동으로 생명 위협	미 FDA Recall/ 체크리스트 1.1/1.3/1.4/1.5/ 1.8/1.9
PM-02		비인가자의 불법 소프트웨어 설치나 실행으로 환자감시장치의 오작동	환자 위험 상황 시 알람 미작동으로 생명 위협	미 FDA Recall/ 체크리스트 1.19
PM-03	정보 위변조	환자감시장치 알람 및 측정 신호 전송 정보의 위변조	환자 위험 상황 시 알람 신호 누락으로 생명 위협	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트1.15/ 1.16/1.17
PM-04		환자감시장치에 저장된 생체신호의 위변조	오진, 잘못 된 치료 수행 또는 치료 기회 박탈	의료기기의 전기·기계적 안전에 관한 공통기준규격 (IEC60601-1) 14.6.1 / 체크리스트 1.17/1.20
PM-05		정보가 알 수 없는 방법으로 암호화 된 경우	치료기회 박탈	미 FDA Recall
PM-06		환자감시장치설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	환자 위험 상황 시 알람 미작동으로 생명 위협	미 FDA Recall

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
PM-07	플래폼 또는 하드웨어 취약	무허가 업데이트	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 1.12
PM-08		무결성이 보장되지 않은 업데이트	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 1.13
PM-09		인증되지 않은 업데이트	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 1.14
PM-10		물리적 통신포트 제공	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 1.18
PM-11		시스템 로그 부재	알람 설정 조작으로 환자 생명 위협	의료기기 이상사례보고 / 체크리스트 2.1
PM-12		무결성이 보장되지 않은 실행파일 및 설정파일	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 2.2
PM-13		사이버 보안 위협 탐지 시 대응책 부재	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 2.3

No.	위해요인 (Hazard)	구체적인 예시	사용자 또는 환자에게 발생가능한 손상	관련자료
PM-14	통신채널 취약	DDoS 공격 방어책 부재	환자 위험 상황 시 알람 미작동으로 생명 위협	의료기기 이상사례보고 / 체크리스트 2.4
…	…	…	…	…

※ 관련 자료 중 미 FDA Recall은 해당 제품 또는 유사 제품의 국외 Recall 사례를 의미함

5.2 각 위해 상황에서의 위험 산정

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
PM-01-01	환자감시장치의 알람 등 설정 메뉴에 비인가 접근으로 기기 설정 조작	접근통제 기능 없이 누구나 환자 감시장치 설정에 접근하도록 한 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협	2	5
PM-01-02		비인가자의 환자 감시장치 접근 시도를 감지하지 못하는 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-01-03		보안이 취약한 공유기 이용으로 사용자 접근 권한이 탈취된 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-01-04		관리자가 설정 완료 후 설정 메뉴 접근을 종료하지 않고 자리를 비웠을 때 비인가자가 이용	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-01-05		접근 권한을 가진 사용자 변경 시 이전 사용자가 비밀번호를 알아 불법 접근	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-02	비인가자의 불법 소프트웨어 설치나 실행으로 환자감시장치의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협		

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
PM-03	환자감시장치 알람 및 측정 신호 전송 정보의 위변조	스니핑을 통한 전송 정보의 유출 및 중간자 공격을 통한 위변조	전송 정보 위변조로 알람 신호 누락	환자 위험 상황 시 알람 신호 누락으로 생명 위협		
PM-04	환자감시장치에 저장된 생체신호의 위변조	중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈		
PM-05	정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈		
PM-06	환자감시장치설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	중간자공격으로 알람이 미작동하도록 설정을 변경하는 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-10	물리적 통신포트 제공	기기에 설치된 디버깅(개발자용) 포트로 기기 접속	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-11	시스템 로그 부재	비인가자가 접속 기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 기기 설정 변경	조작 된 설정으로 중 환자 모니터링	알람 설정 조작으로 환자 생명 위협		
PM-12	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		

No.	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성
PM-13	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응 절차가 부재한 상황에서 보안사고 발생 유도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		
PM-14	DDoS 공격 방어책 부재	네트워크 접속 가능한 의료기기에 지속적인 공격 트래픽 전송, 의료기기가 연결된 네트워크장비에 지속적이고 대용량의 공격 트래픽을 전송하여 네트워크 무력화	환자 모니터링 정보 전송 불가	환자 위험 상황 시 알람 미작동으로 생명 위협		
...	...	...	...	...	...	...

※ 발생가능성 및 심각성은 위험관리계획서에 정의된 기준에 따라 평가한다.

6. 위험평가

※ 심각성 및 발생가능성 평가기준은 위험관리계획서에서 정의된 기준에 따라 기재한다.

6.1 심각성 평가기준

용어	단계	가능한 기술
치명적	5	심각한 상해, 사망
높음	4	신체기능의 영구적 장애 또는 신체 구조의 영구적 손상
중간	3	일시적이고 경미한 상해, 의학적 중재 필요
낮음	2	일시적인 불편, 의학적 중재 없이 가역적
무시	1	경미하고 단시간 불편

6.2 발생가능성 평가기준

용어	단계	정의 (p=판매건수를 척도로 한 발생건수)
상습적 발생 (Frequent)	6	1/10 ≦ P
자주 발생 (Probable)	5	1/50 ≦ P < 1/10
가끔 발생(Occasional)	4	1/200 ≦ P < 1/50
이따끔 발생 (Remote)	3	1/350 ≦ P < 1/200
희박한 발생 (Improbable)	2	1/500 ≦ P < 1/350
발생가능 거의없는 (Incredible)	1	P<1/500

6.3 위험 허용 판정

상습적 발생	6	6	12	18	24	30
자주 발생	5	5	10	15	20	25
가끔 발생	4	4	8	12	16	20
이따끔 발생	3	3	6	9	12	15
희박한 발생	2	2	4	6	8	10
발생가능 거의없는	1	1	2	3	4	5
		무시 1	낮은 2	중간 3	높음 4	침명적 5

- 수락(널리 허용 가능한 영역, Acceptable risk, Green Zone) Level 0~4
- 중간(합리적으로 실현할 수 있는 가장 낮은(ALARP) 영역, As Low As Reasonably Practicable, Yellow Zone) Level 5~11
- 비수락(허용할 수 없는 영역, Unacceptable risk, Red Zone) Level 12~30

6.4 위험평가

No.	위험분석(Risk analysis)						위험평가 (Risk evaluation)	
	위해요인 (Hazard)	발생 가능한 사례	위해상황 (Hazard situation)	위해 (Harm)	발생 가능성	심각성	위험	결과
PM-01-01	환자감시장치의 알람 등 설정 메뉴에 비인가 접근으로 기기 설정 조작	접근통제 기능 없이 누구나 환자감시장치 설정에 접근하도록 한 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협	3	5	15	비수락

PM-01-02		비인가자의 환자감시장치 접근 시도를 감지하지 못하는 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-01-03		보안이 취약한 공유기 이용으로 사용자 접근 권한이 탈취된 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-01-04		관리자가 설정 완료 후 설정 메뉴 접근을 종료하지 않고 자리를 비웠을 때 비인가자가 이용	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-01-05		접근 권한을 가진 사용자 변경 시 이전 사용자가 비밀번호를 알아 불법 접근	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-02	비인가자의 불법 소프트웨어 설치나 실행으로 환자감시장치의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-03	환자감시장치 알람 및 측정 신호 전송 정보의 위변조	스니핑을 통한 전송 정보의 유출 및 중간자 공격을 통한 위변조	전송 정보 위변조로 알람 신호 누락	환자 위험 상황 시 알람 신호 누락으로 생명 위협				
PM-04	환자감시장치에 저장된 생체신호의 위변조	중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못 된 치료 수행 또는 치료 기회 박탈				
PM-05	정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈				
PM-06	환자감시장치 설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	중간자공격으로 알람이 미작동하도록 설정을 변경하는 경우	조작 된 설정으로 중 환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협				

PM-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-10	물리적 통신포트 제공	기기에 설치된 디버깅(개발자용) 포트로 기기 접속	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-11	시스템 로그 부재	비인가자가 접속기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 기기 설정 변경	조작 된 설정으로 중환자 모니터링	알람 설정 조작으로 환자 생명 위협				
PM-12	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-13	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
PM-14	DDoS 공격 방어책 부재	네트워크 접속 가능한 의료기기에 지속적인 공격 트래픽 전송 의료기기가 연결된 네트워크장비에 지속적이고 대용량의 공격 트래픽을 전송하여 네트워크 무력화	환자 모니터링 정보 전송 불가	환자 위험 상황 시 알람 미작동으로 생명 위협				
…	…	…	…	…	…	…	…	…

※ 위험관리계획서에 정의된 기준에 따라 발생가능성 및 심각성, 위험, 결과를 평가한다.

7. 위험통제

7.1 위험통제 조치

No.	위험통제 조치 (Risk Control)	위험통제 조치 실행	잔여위험평가			결과	위험/이득분석	추가발생위험	통제완료
			발생가능성	심각성	위험				
PM-RC-01-01	설계 변경을 통한 설정메뉴에 접근 통제 및 인증 기능 구현	소프트웨어 검증 자료로 접근통제 및 인증 기능 구현 확인	1	5	5	중간	Y	N	Y
PM-RC-01-02	설계 변경을 통한 비인가자의 접근 시도 시 설정 메뉴 접근 제한 기능 구현	소프트웨어 검증 자료로 비인가자의 접근 시도 시 설정 메뉴 접근제한 기능 구현 확인							
PM-RC-01-03	설계 변경을 통한 네트워크를 통한 접속시 인증 기능 구현	소프트웨어 검증 자료로 네트워크를 통한 접속시 인증 기능 구현 확인							
PM-RC-01-04	설계 변경을 통한 설정 메뉴 세션 자동종료 기능 구현	소프트웨어 검증 자료로 세션 자동종료 기능 구현 확인							
PM-RC-01-05	설계 변경을 통한 주기적 비밀번호 변경 기능 구현 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공	소프트웨어 검증 자료로 주기적 비밀번호 변경 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공 확인							
PM-RC-02	설계 변경을 통한 불필요한 서비스 비활성화	소프트웨어 검증 자료로 불필요한 서비스 비활성화 확인							
PM-RC-03	설계 변경을 통한 전송 정보의 암호화 기능 구현	소프트웨어 검증 자료로 전송 정보의 암호화 기능 구현 확인							
PM-RC-04	설계 변경을 통한 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현	소프트웨어 검증 자료로 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현 확인							
PM-RC-05	설계 변경을 통한 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현	소프트웨어 검증 자료로 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현 확인							
PM-RC-06	설계 변경을 통한 원격 설정 기능 차단 기능 구현	소프트웨어 검증 자료로 원격 설정 기능 차단 구현 확인							

PM-RC-07	설계 변경을 통한 업데이트 시 인증 기능 구현	소프트웨어 검증 자료로 업데이트 시 인증 기능 구현 확인							
PM-RC-08	설계 변경을 통한 업데이트 시 무결성 체크 기능 구현	소프트웨어 검증 자료로 업데이트 시 무결성 체크 기능 구현 확인							
PM-RC-09	설계 변경을 통한 업데이트 제공자 인증 절차 기능 구현	소프트웨어 검증 자료로 업데이트 제공자 인증 절차 기능 구현 확인							
PM-RC-10	물리적 통신포트 잠금 혹은 제거	물리적 통신포트 제공여부 확인							
PM-RC-11	설계 변경을 통한 시스템 접속 및 정보 관리 로그 기능 구현	소프트웨어 검증 자료로 시스템 접속 및 정보 관리 로그 기능 구현 확인							
PM-RC-12	설계 변경을 통한 실행파일 실행전 무결성 체크 기능 구현	소프트웨어 검증 자료로 실행파일 실행전 무결성 체크 기능 구현 확인							
PM-RC-13	설계 변경을 통한 보안 위협 탐지 알람 기능 구현 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 보안 위협 탐지 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인							
PM-RC-14	사용자매뉴얼을 통해 사용자에게 분리 된 내부망 구축 절차 제공 ※ 예시 의료기관내 VPN을 이용하여 망 분리된 네트워크 환경에서 시스템을 구축한다.	사용자매뉴얼을 통해 사용자 구축 절차 제공 확인							
…	…	…	…	…	…	…	…	…	…

※ 위험관리계획서에 정의된 기준에 따라 발생가능성 및 심각성, 위험, 결과, 위험/이득분석, 추가발생위험, 통제완료를 평가한다.

7.2 위험통제 조치 설명

No.	위험통제 조치(Risk Control)	위험통제 조치 설명
PM-RC-01-01	설정메뉴 접근통제 및 인증 기능	설정 메뉴 접근 시 인증번호를 입력하도록 구현한다.
PM-RC-01-02	비인가자의 접근 감지 및 제한 기능	잘못 된 PW를 이용하여 지속적인 로그인 시도에 대해 감지하는 기능을 구현하고 PW를 5회이상 잘못 입력하면 해당 메뉴의 접속을 제한한다.
PM-RC-01-03	네트워크를 통한 접속시 인증 기능	네트워크의 인증정보를 확인하여 접속한다.
PM-RC-01-04	설정 메뉴 세션 자동종료 기능	접속 후 10분간 활동이 없으면 접속을 종료한다.
PM-RC-01-05	주기적 비밀번호 변경 기능 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공	PW는 3개월 주기로 변경을 알리는 메세지를 제공하고 관리 상 주의사항을 제공한다.
PM-RC-02	불필요한 서비스 비활성화	불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 유지보수를 위한 포트는 IP를 제한하여 접속한다.
PM-RC-03	전송 정보의 암호화 기능	의료영상, 개인의료정보 전송시 OO프로토콜을 이용하여 암호화한다.
PM-RC-04	중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능	생체정보는 임시 저장 후 전송 시 삭제한다.
PM-RC-05	중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능	생체정보는 임시 저장 후 전송 시 삭제한다.
PM-RC-06	원격 설정 기능 차단 기능	기기 설정 메뉴는 오프라인으로만 접근하도록 한다.
PM-RC-07	업데이트 시 인증 기능	펌웨어 또는 소프트웨어 업데이트 시 관리자의 인가를 요청 및 확인하는 절차를 구현한다.
PM-RC-08	업데이트 시 무결성 체크 기능	펌웨어 또는 소프트웨어 업데이트 파일의 무결성을 체크하는 기능을 구현한다.
PM-RC-09	업데이트 제공자 인증 절차 기능	펌웨어 또는 소프트웨어의 업데이트 시 인증된 코드로 제한 한다.
PM-RC-10	물리적 통신포트 잠금 혹은 제거	펌웨어 업데이트를 위한 포트는 출고 시 비활성화 한다.
PM-RC-11	시스템 접속 및 정보 관리 로그 기능	사용자의 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등 로그 정보를 기록한다.

PM-RC-12	실행파일 실행전 무결성 체크 기능	실행파일 및 설정파일에 대한 무결성을 체크하는 기능을 구현한다.
PM-RC-13	보안 위협 탐지 알람 기능 사용자매뉴얼을 통해 사용자에 대응 절차 제공	보안 위협에 따른 통신 오류, 지연 등, 기기 설정 변경, 비인가 접속 등을 탐지하여 사용자에게 알람을 제공한다. 이에 대한 제조자 담당자 연락처를 매뉴얼에 제공하고, 사이버 보안 위협 탐지 시 취해야 할 대응책 사용자에게 제공 한다.
PM-RC-14	의료기관내 VPN을 이용하여 망 분리된 네트워크 환경에서 시스템을 구축 한다.	의료기관내에 환자감시장치에 대한 네트워크를 분리(물리 or 논리적 망 분리)하고, DDoS 방어 전용장비 설치를 통해 탐지/방어를 지원하는 네트워크 시스템을 구축한다.
		-
		-
		-

8. 전체 잔여위험 허용가능성 평가

No.	잔여 위험평가			결과	위험/이득 분석	추가 발생 위험	통제 완료	전체 잔여위험 허용가능성 평가 (Evaluation of overall residual risk acceptability)
	발생 가능성	심각성	위험					허용가능 /허용불가
PM-RC-01-01	**1**	**5**	**5**	**중간**	**Y**	**N**	**Y**	**허용가능**
PM-RC-01-02								
PM-RC-01-03								
PM-RC-01-04								
PM-RC-01-05								
PM-RC-02								
PM-RC-03								
PM-RC-04								
PM-RC-05								

PM-RC-06								
PM-RC-07								
PM-RC-08								
PM-RC-09								
PM-RC-10								
PM-RC-11								
PM-RC-12								
PM-RC-13								
...								

9. 위험관리보고서

※ 위험관리보고서는 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

10. 생산 및 생산 후 정보 입수를 위한 방법

※ 생산 및 생산 후 정보 입수를 위한 방법은 「의료기기 위험관리 가이드라인(2007)」에 따르며, 사이버 보안 측면에서 추가적으로 고려가 필요한 사항이 없으므로 본 예시에서 생략한다.

11. FMEA 보고서

No.	위험분석 (Risk analysis)						위험 평가 (Risk evaluation)		위험통제 (Risk control)								전체 잔여 위험 허용 가능성 평가
	위해 요인	발생 가능한 사례	위해상황	위해	발생가능성	심각성	위험	결과	위험통제조치	위험통제조치 실행	발생가능성	심각성	위험	결과	위험이득분석	추가발생위험	통제완료	허용 가능 / 허용 불가
PM-01-01	환자감시장치의 알람 등 설정 메뉴에 비인가 접근으로 기기 설정 조작	접근통제 기능 없이 누구나 환자 감시장치 설정에 접근하도록 한 경우	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협	3	5	15	비수락	설계 변경을 통한 설정메뉴에 접근통제 및 인증 기능 구현	소프트웨어 검증 자료로 접근통제 및 인증 기능 구현 확인	1	5	5	중간	Y	N	Y	허용 가능
PM-01-02		비인가자의 환자감시장치 접근 시도를 감지하지 못하는 경우	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 비인가자의 접근 시도 시 설정 메뉴 접근 제한 기능 구현	소프트웨어 검증 자료로 비인가자의 접근 시도 시 설정 메뉴 접근제한 기능 구현 확인								
PM-01-03		보안이 취약한 공유기 이용으로 사용자 접근 권한이 탈취된 경우	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 네트워크를 통한 접속시 인증 기능 구현	소프트웨어 검증 자료로 네트워크를 통한 접속시 인증 기능 구현 확인								
PM-01-04		관리자가 설정 완료 후 설정 메뉴 접근을 종료하지 않고 자리를 비웠을 때 비인가자가 이용	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 설정 메뉴 세션 자동종료 기능 구현	소프트웨어 검증 자료로 세션 자동 종료 기능 구현 확인								

PM-01-05		접근 권한을 가진 사용자 변경 시 이전 사용자가 비밀번호를 알아 불법 접근	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 주기적 비밀번호 변경 기능 구현 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공	소프트웨어 검증 자료로 주기적 비밀번호 변경 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 비밀번호 관리 주의 제공 확인								
PM-02	비인가자의 불법 소프트웨어 설치나 실행으로 환자감시장치의 오작동	외부 네트워크로부터 기기에서 활성화 된 통신 서비스를 통해 접속	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 불필요한 서비스 비활성화	소프트웨어 검증 자료로 불필요한 서비스 비활성화 확인								
PM-03	환자감시장치 알람 및 측정 신호 전송 정보의 위변조	스니핑을 통한 전송 정보의 유출 및 중간자 공격을 통한 위변조	전송 정보 위변조로 알람 신호 누락	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 전송 정보의 암호화 기능 구현	소프트웨어 검증 자료로 전송 정보의 암호화 기능 구현 확인								
PM-04	환자감시장치에 저장된 생체신호의 위변조	중간자 공격을 통한 위변조	조작 된 정보로 진료 수행	오진, 잘못된 치료 수행 또는 치료 기회 박탈					설계 변경을 통한 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현	소프트웨어 검증 자료로 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현 확인								
PM-05	정보가 알 수 없는 방법으로 암호화 된 경우	랜섬웨어 감염	진료 시 환자 정보 열람 불가	치료기회 박탈					설계 변경을 통한 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현	소프트웨어 검증 자료로 중앙감시장치로 정보 전송 시 임시저장 정보 삭제 기능 구현 확인								

PM-06	환자감시장치설정 정보에 변경이 발생하였으나, 해당 발생여부를 확인할 수 없는 경우	중간자공격으로 알람이 미작동하도록 설정을 변경하는 경우	조작 된 설정으로 중환자 모니터링 시 알람 미작동	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 원격 설정 기능 차단 기능 구현	소프트웨어 검증 자료로 원격 설정 기능 차단 구현 확인								
PM-07	무허가 업데이트	관리자의 허가 없이 펌웨어 및 소프트웨어 업데이트 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 업데이트 시 인증 기능 구현	소프트웨어 검증 자료로 업데이트 시 인증 기능 구현 확인								
PM-08	무결성이 보장되지 않은 업데이트	위변조된 펌웨어나 소프트웨어를 이용한 업데이트 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 업데이트 시 무결성 체크 기능 구현	소프트웨어 검증 자료로 업데이트 시 무결성 체크 기능 구현 확인								
PM-09	인증되지 않은 업데이트	인증절차 없이 임의의 제공자로부터 펌웨어나 소프트웨어 업데이트	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 업데이트 제공자 인증 절차 기능 구현	소프트웨어 검증 자료로 업데이트 제공자 인증 절차 기능 구현 확인								
PM-10	물리적 통신포트 제공	기기에 설치된 디버깅(개발자용) 포트로 기기 접속	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					물리적 통신 포트 잠금 혹은 제거	물리적 통신포트 제공여부 확인								
PM-11	시스템 로그 부재	비인가자가 접속 기록에 관계없이 기기 접속 혹은 추적이 불가능한 상태에서 기기 설정 변경	조작 된 설정으로 중환자 모니터링	알람 설정 조작으로 환자 생명 위협					설계 변경을 통한 시스템 접속 및 정보 관리 로그 기능 구현	소프트웨어 검증 자료로 시스템 접속 및 정보 관리 로그 기능 구현 확인								

PM-12	무결성이 보장되지 않은 실행파일 및 설정파일	악성코드를 포함한 실행파일(펌웨어, OS, SW)을 업로드하여 기기 작동 시도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 실행파일 실행전 무결성 체크 기능 구현	소프트웨어 검증 자료로 실행파일 실행전 무결성 체크 기능 구현 확인								
PM-13	사이버 보안 위협 탐지 시 대응책 부재	사이버 보안 위협 발생 시 대응절차가 부재한 상황에서 보안사고 발생 유도	환자 진료 시 기기 오작동으로 모니터링 수행 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					설계 변경을 통한 보안 위협 탐지 알람 기능 구현 및 사용자 매뉴얼을 통해 사용자에 대응 절차 제공	소프트웨어 검증 자료로 보안 위협 탐지 알람 기능 구현 확인 및 사용자매뉴얼을 통해 사용자에 대응 절차 제공 확인								
PM-14	DDoS 공격 방어책 부재	네트워크 접속 가능한 의료기기에 지속적인 공격 트래픽 전송, 의료기기가 연결된 네트워크장비에 지속적이고 대용량의 공격 트래픽을 전송하여 네트워크 무력화	환자 모니터링 정보 전송 불가	환자 위험 상황 시 알람 미작동으로 생명 위협					사용자 매뉴얼을 통해 사용자에게 분리된 내부망 구축절차 제공	사용자 매뉴얼을 통해 사용자 구축 절차 제공 확인								
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

2. 필수원칙 체크리스트 적용사례

아래는 ‘2등급 유헬스케어 게이트웨이’, ‘범용초음파영상진단장치’, ‘환자감시장치’의 의료기기 사이버 보안 필수원칙 체크리스트 적용사례다.

해당 예시는 위 Ⅲ-1의 각 제품별 위험관리 보고서 적용사례를 기반으로 작성한 것으로 반드시 이를 따라야 하는 것은 아니며, 제품의 특성에 따라 각 항목의 내용이 달라질 수 있다.

가. 2등급 유헬스케어 게이트웨이

< 의료기기 사이버 보안 특성 기재 >

1) 사이버 보안 안전성 등급 : □상 ■중 □하

2) 사용되는 통신 기술 : Bluetooth Low Energy, 3G, LTE, Wi-Fi

3) 통신목적 : ■ 환자의 생체정보 등의 개인의료정보 송수신
□ 기기제어
■ 펌웨어 또는 소프트웨어 업데이트 등 유지보수

4) 공용 네트워크망 사용여부 : 사용

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
2. 식별 및 보호				
1.1 접근통제 및 인증 식별 및 인증에 기반하여 사용자(의료기기) 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.	적용	성능 시험	‘IEC 62304’ ‘스마트의료 사이버보안 가이드’ ‘사물인터넷 보안 시험·인증 기준 해설서’	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.2 다중접속 금지 동일 사용자가 다중으로 접속하지 않아야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.3 사용자(의료기기) 접속 인식 비인가된 사용자(의료기기)가 접속될 시 이를 인식하여 구분할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.4 비인가된 사용자(의료기기) 접속 제한 비인가된 사용자(의료기기)의 접속 시 접속을 제한할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.5 비인가된 네트워크 통신 차단 비인가된 네트워크 통신 접속을 제한할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.6 원격접속 차단 사용자(의료기기)가 의료기관의 서버에 접속할 수 있는 경우, 사용자 계정 또는 의료기기 도난 시 해당 계정(의료기기)이 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.7 사용자(의료기기) 인증 관리 사용자(의료기기) 계정의 유효기간을 설정할 수 있어야 하며, 설정된 유효기간 만료 시 접근이 통제되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.8 자동세션종료 설정된 시간 이후에는 의료기기간의 통신 또는 접속이 종료되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.9 비밀번호 작성 규칙 강화 비밀번호 작성규칙은 '개인정보의 기술적·관리적 보호조치 기준'을 만족하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.10 비밀번호 하드코딩 금지 비밀번호를 하드코딩하지 않아야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.11 비밀번호 노출 금지 비밀번호를 입력 시 ***와 같이 노출되지 않는 형태로 사용되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.12 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.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.13 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.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.14 펌웨어 또는 소프트웨어 업데이트 시 인증 방식 사용 펌웨어 또는 소프트웨어의 업데이트 시 코드 서명 확인 등 인증된 코드로 제한하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.15 네트워크상의 의료기기 제어정보 전송 기밀성 및 무결성 보장 네트워크를 통하여 의료기기 제어정보를 주고받을 경우 적절한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	해당없음	원격 제어기능 없음		
1.16 네트워크 상의 개인의료정보 전송 기밀성 및 무결성 보장 네트워크를 통하여 개인의료정보를 주고받을 경우 적절한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.17 안전한 암호 알고리즘 사용 데이터 전송 및 저장 시 사용되는 암호 알고리즘은 112비트 이상 보안강도를 가진 검증된 암호 알고리즘 또는 모듈을 사용하여야하며, 암호화 시 사용되는 암호키는 안전하게 관리되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.18 물리적인 통신포트 침해의 최소화 통신포트의 침해를 최소화하기 위해 기기에 물리적인 잠금을 제공하여야 한다.	해당없음	모바일 의료용앱으로 물리적 단말기 없음		
1.19 불필요한 서비스 비활성화 불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 외부 접속 포트를 사용할 경우 비밀번호 설정, IP 제한 등의 추가적인 보안 조치를 수행하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.20 개인의료정보 저장관리 의료기관 외부에서 사용되는 측정기기 또는 게이트웨이에는 개인의료정보를 저장하지 않는 것을 권고한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
2. 탐지, 대응, 복구				
2.1 데이터 감사를 위한 시스템 로그 기록 사용자의 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등과 같은 로그가 기록되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
2.2 주요 실행파일 및 설정파일에 대한 무결성 검증 및 대응 의료기기의 정상 작동을 보장하기 위해 주요 실행파일 및 설정파일에 대한 무결성을 검증하여야 하며, 무결성 오류 발생 시 대응방안을 고려하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
2.3 사이버 보안 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 제공하여야 하며, 사이버 보안 위협 탐지 시 취해야 할 대응책을 수립하고 사용자에게 제공하여야 한다.	적용	성능 시험 정보 제공 관련 규정	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194) 사용설명서 (IFU-001)
2.4 DDoS 공격에 대한 방어 공용 네트워크망에 접속하여 의료기기를 실시간으로 제어 또는 환자 생명과 직접적으로 연관될 수 있는 정보(예: 사이버 보안 안전성 등급 '상'에 해당되는 정보 등)를 실시간으로 송수신하는 장비의 경우 DDoS 공격에 대한 대응책이 수립되어야 한다.	해당없음	만성진환자의 혈압 값을 수집해서 병원으로 송신하는 제품으로서 앱 형태이고, 실시간 감시 목적으로는 사용되지 않는 제품임		

나. 범용초음파영상진단장치

< 의료기기 사이버 보안 특성 기재 >

1) 사이버 보안 안전성 등급 : □상 ■중 □하

2) 사용되는 통신 기술 : 유선 LAN

3) 통신목적 : □ 환자의 생체정보 등의 개인의료정보 송수신

□ 기기제어

■ 펌웨어 또는 소프트웨어 업데이트 등 유지보수

4) 공용 네트워크망 사용여부 : 사용

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
3. 식별 및 보호				
1.1 접근통제 및 인증 식별 및 인증에 기반하여 사용자(의료기기) 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.2 다중접속 금지 동일 사용자가 다중으로 접속하지 않아야 한다.	해당없음	네트워크를 통해 접근하는 별도 계정 없음		
1.3 사용자(의료기기) 접속 인식 비인가된 사용자(의료기기)가 접속될 시 이를 인식하여 구분할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.4 비인가된 사용자(의료기기) 접속 제한 비인가된 사용자(의료기기)의 접속 시 접속을 제한할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.5 비인가된 네트워크 통신 차단 비인가된 네트워크 통신 접속을 제한할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.6 원격접속 차단 사용자(의료기기)가 의료기관의 서버에 접속할 수 있는 경우, 사용자 계정 또는 의료기기 도난 시 해당 계정(의료기기)이 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다.	해당없음	원격 접속 계정 없음		
1.7 사용자(의료기기) 인증 관리 사용자(의료기기) 계정의 유효기간을 설정할 수 있어야 하며, 설정된 유효기간 만료 시 접근이 통제되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.8 자동세션종료 설정된 시간 이후에는 의료기기간의 통신 또는 접속이 종료되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.9 비밀번호 작성 규칙 강화 비밀번호 작성규칙은 '개인정보의 기술적·관리적 보호조치 기준'을 만족하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.10 비밀번호 하드코딩 금지 비밀번호를 하드코딩하지 않아야 한다.	해당없음	원격 접속 계정 없음		
1.11 비밀번호 노출 금지 비밀번호를 입력 시 ***와 같이 노출되지 않는 형태로 사용되어야 한다.	해당없음	원격 접속 계정 없음		
1.12 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.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.13 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.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.14 펌웨어 또는 소프트웨어 업데이트 시 인증 방식 사용 펌웨어 또는 소프트웨어의 업데이트 시 코드 서명 확인 등 인증된 코드로 제한하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.15 네트워크상의 의료기기 제어정보 전송 기밀성 및 무결성 보장 네트워크를 통하여 의료기기 제어정보를 주고받을 경우 적절한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	해당없음	원격 제어기능 없음		
1.16 네트워크 상의 개인의료정보 전송 기밀성 및 무결성 보장 네트워크를 통하여 개인의료정보를 주고받을 경우 적절한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.17 안전한 암호 알고리즘 사용 데이터 전송 및 저장 시 사용되는 암호 알고리즘은 112비트 이상 보안강도를 가진 검증된 암호 알고리즘 또는 모듈을 사용하여야하며, 암호화 시 사용되는 암호키는 안전하게 관리되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.18 물리적인 통신포트 침해의 최소화 통신포트의 침해를 최소화하기 위해 기기에 물리적인 잠금을 제공하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.19 불필요한 서비스 비활성화 불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 외부 접속 포트를 사용할 경우 비밀번호 설정, IP 제한 등의 추가적인 보안 조치를 수행하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.20 개인의료정보 저장관리 의료기관 외부에서 사용되는 측정기기 또는 게이트웨이에는 개인의료정보를 저장하지 않는 것을 권고한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
2. 탐지, 대응, 복구				
2.1 데이터 감사를 위한 시스템 로그 기록 사용자의 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등과 같은 로그가 기록되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
2.2 주요 실행파일 및 설정파일에 대한 무결성 검증 및 대응 의료기기의 정상 작동을 보장하기 위해 주요 실행파일 및 설정파일에 대한 무결성을 검증하여야 하며, 무결성 오류 발생 시 대응방안을 고려하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
2.3 사이버 보안 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 제공하여야 하며, 사이버 보안 위협 탐지 시 취해야 할 대응책을 수립하고 사용자에게 제공하여야 한다.	적용	성능 시험 정보 제공 관련 규정	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194) 사용설명서 (IFU-001)
2.4 DDoS 공격에 대한 방어 공용 네트워크망에 접속하여 의료기기를 실시간으로 제어 또는 환자 생명과 직접적으로 연관될 수 있는 정보(예: 사이버 보안 안전성 등급 '상'에 해당되는 정보 등)를 실시간으로 송수신하는 장비의 경우 DDoS 공격에 대한 대응책이 수립되어야 한다.	해당없음	진료시 내부 폐쇄망으로 시스템 구현 및 통신 미이용		

다. 환자감시장치

< 의료기기 사이버 보안 특성 기재 >

1) 사이버 보안 안전성 등급 : ■상 □중 □하

2) 사용되는 통신 기술 : 유선 LAN, USB

3) 통신목적 : □ 환자의 생체정보 등의 개인의료정보 송수신

□ 기기제어

■ 펌웨어 또는 소프트웨어 업데이트 등 유지보수

4) 공용 네트워크망 사용여부 : 사용

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
4. 식별 및 보호				
1.1 접근통제 및 인증 식별 및 인증에 기반하여 사용자(의료기기) 역할에 따른 접근 권한을 부여가 가능하고 접근 권한에 따라 인가된 데이터에만 접근 가능해야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.2 다중접속 금지 동일 사용자가 다중으로 접속하지 않아야 한다.	해당없음	네트워크를 통해 접근하는 별도 계정 없음		
1.3 사용자(의료기기) 접속 인식 비인가된 사용자(의료기기)가 접속될 시 이를 인식하여 구분할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.4 비인가된 사용자(의료기기) 접속 제한 비인가된 사용자(의료기기)의 접속 시 접속을 제한할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.5 비인가된 네트워크 통신 차단 비인가된 네트워크 통신 접속을 제한할 수 있어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.6 원격접속 차단 사용자(의료기기)가 의료기관의 서버에 접속할 수 있는 경우, 사용자 계정 또는 의료기기 도난 시 해당 계정(의료기기)이 서버에 접속할 수 없도록 접근통제를 할 수 있어야 한다.	해당없음	원격 접속 계정 없음		
1.7 사용자(의료기기) 인증 관리 사용자(의료기기) 계정의 유효기간을 설정할 수 있어야 하며, 설정된 유효기간 만료 시 접근이 통제되어야 한다.	해당없음	설정 메뉴 접근 통제 기능 외 별도 계정없음		
1.8 자동세션종료 설정된 시간 이후에는 의료기기간의 통신 또는 접속이 종료되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.9 비밀번호 작성 규칙 강화 비밀번호 작성규칙은 '개인정보의 기술적·관리적 보호조치 기준'을 만족하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.10 비밀번호 하드코딩 금지 비밀번호를 하드코딩하지 않아야 한다.	해당없음	원격 접속 계정 없음		
1.11 비밀번호 노출 금지 비밀번호를 입력 시 ***와 같이 노출되지 않는 형태로 사용되어야 한다.	해당없음	원격 접속 계정 없음		
1.12 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.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.13 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.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.14 펌웨어 또는 소프트웨어 업데이트 시 인증 방식 사용 펌웨어 또는 소프트웨어의 업데이트 시 코드 서명 확인 등 인증된 코드로 제한하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.15 네트워크상의 의료기기 제어정보 전송 기밀성 및 무결성 보장 네트워크를 통하여 의료기기 제어정보를 주고받을 경우 적절한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	해당없음	원격 제어기능 없음		
1.16 네트워크 상의 개인의료정보 전송 기밀성 및 무결성 보장 네트워크를 통하여 개인의료정보를 주고받을 경우 적절한 암호화 및 복호화 방식을 활용하여 기밀성과 무결성을 보장하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.17 안전한 암호 알고리즘 사용 데이터 전송 및 저장 시 사용되는 암호 알고리즘은 112비트 이상 보안강도를 가진 검증된 암호 알고리즘 또는 모듈을 사용하여야하며, 암호화 시 사용되는 암호키는 안전하게 관리되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
1.18 물리적인 통신포트 침해의 최소화 통신포트의 침해를 최소화하기 위해 기기에 물리적인 잠금을 제공하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.19 불필요한 서비스 비활성화 불필요한 외부 접속 포트 등의 서비스 비활성화를 기본값으로 설정하고, 외부 접속 포트를 사용할 경우 비밀번호 설정, IP 제한 등의 추가적인 보안 조치를 수행하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
1.20 개인의료정보 저장관리 의료기관 외부에서 사용되는 측정기기 또는 게이트웨이에는 개인의료정보를 저장하지 않는 것을 권고한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
2. 탐지, 대응, 복구				
2.1 데이터 감사를 위한 시스템 로그 기록 사용자의 의료기기에 접속 시 접속기록, 환자정보 조회, 데이터 생성, 변경, 삭제 등과 같은 로그가 기록되어야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준	시험보고서 (MK-1194)

사이버 보안 필수원칙	해당기기 적용여부	적합성 입증 방법	해당 법규 및 규격	해당 첨부자료 또는 문서번호
			해설서'	
2.2 주요 실행파일 및 설정파일에 대한 무결성 검증 및 대응 의료기기의 정상 작동을 보장하기 위해 주요 실행파일 및 설정파일에 대한 무결성을 검증하여야 하며, 무결성 오류 발생 시 대응방안을 고려하여야 한다.	적용	성능 시험	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194)
2.3 사이버 보안 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 제공하여야 하며, 사이버 보안 위협 탐지 시 취해야 할 대응책을 수립하고 사용자에게 제공하여야 한다.	적용	성능 시험 정보 제공 관련 규정	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	시험보고서 (MK-1194) 사용설명서 (IFU-001)
2.4 DDoS 공격에 대한 방어 공용 네트워크망에 접속하여 의료기기를 실시간으로 제어 또는 환자 생명과 직접적으로 연관될 수 있는 정보(예: 사이버 보안 안전성 등급 '상'에 해당되는 정보 등)를 실시간으로 송수신하는 장비의 경우 DDoS 공격에 대한 대응책이 수립되어야 한다.	적용	DDoS 공격에 대한 대응책 관련 문서	'IEC 62304' '스마트의료 사이버보안 가이드' '사물인터넷 보안 시험·인증 기준 해설서'	사용설명서 (IFU-001)

의료기기의 사이버 보안 적용방법 및 사례집(민원인 안내서)

발 행 처 식품의약품안전처 식품의약품안전평가원

발 행 일 2019년 11월 28일

발 행 인 이동희

편 집 위 원 장 오현주

편 집 위 원 이정림, 강영규, 정승환, 김수연, 손승호, 한영민, 김건소, 박세일, 김미선, 김미혜

우)28159
충북 청주시 흥덕구 오송읍 오송생명 2로 187

문 의 처 식품의약품안전평가원 첨단의료기기과

전화: 043-719-3908
팩스: 043-719-3900

28159 충북 청주시 흥덕구 오송읍 오송생명2로 187
오송보건의료행정타운
식품의약품안전처 식품의약품안전평가원
의료기기심사부 첨단의료기기과
TEL : 043)719-3908 FAX : 043)719-3900
http://www.mfds.go.kr/medicaldevice

식품의약품안전처
식품의약품안전평가원