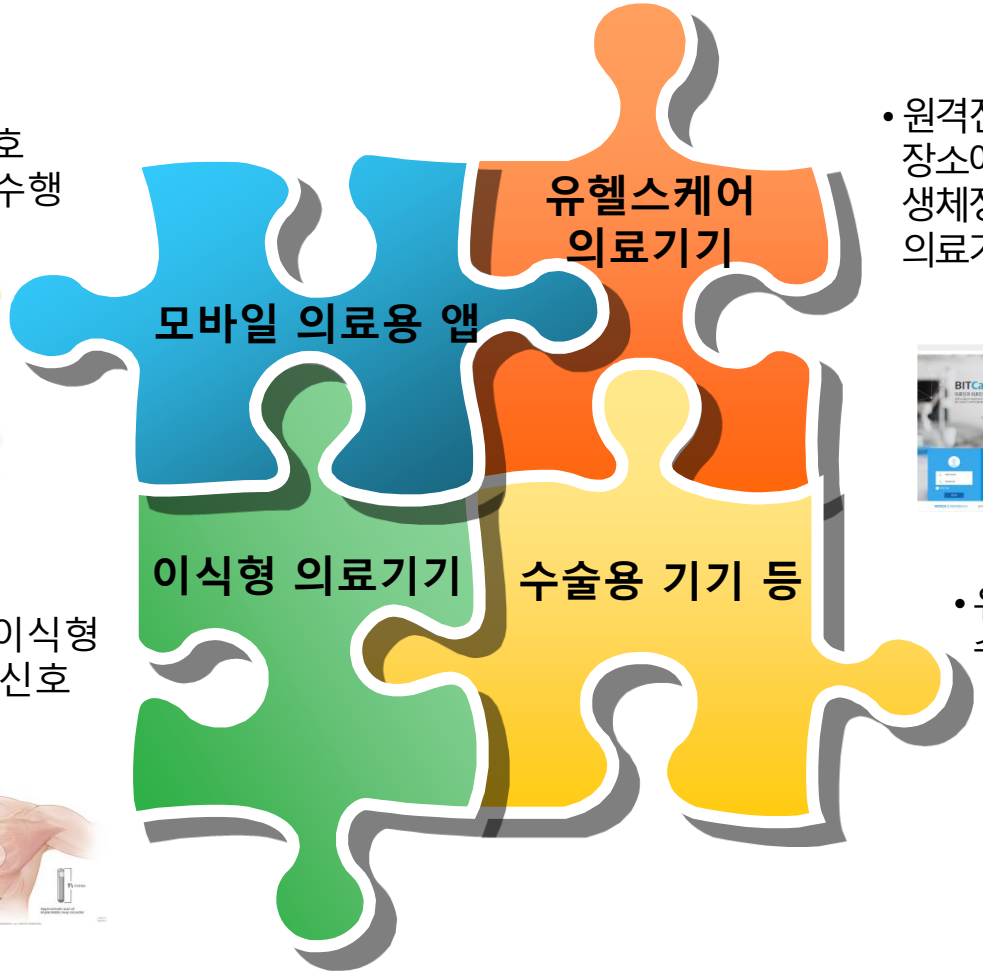
국민 안심이 기준입니다
YOUR SAFETY IS OUR STANDARD

의료기기 사이버보안 적용 및 심사 사례

식품의약품안전처

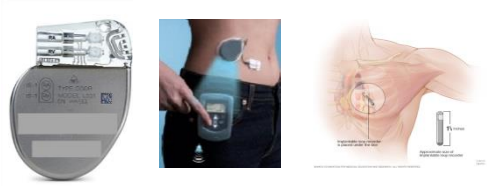
가이드라인 개발 배경 – 통신 기반 의료기기 개발 동향

- 모바일 앱을 이용하여 개인의료정보, 생체신호 송수신, 기기 제어 등 수행



- 원격진료를 위해 의료기관 이외의 장소에서 개인의료정보 및 생체정보를 측정수집하고 의료기관에 전송·저장함

- 무선통신을 이용하여 이식형 의료기기의 정보, 생체신호 등 송수신, 기기 제어



- 유무선 통신을 이용하여 수술용 기기를 제어

가이드라인 개발 배경 - 국내·외 사건 동향

심장이식 관련 의료기기 해킹할 수 있는 보안취약점 발견돼

김민권 기자 | 승인 2020.12.16 18:39

IoT 보안 회사 스터넘 보안전문가들이 페어링 된 심장 장치를 제어하기 위해 사용되는 메드트로닉사의 'MyCareLink Smart 25000 Patient Reader' 제품에서 보안취약점이 발견됐다고 밝혔다.

HOME > 해외 > 의료기기

美 메드트로닉 인슐린 펌프 리콜

미니메드 508과 패러다임, 사이버보안 취약

김자연 기자 승인 2019.06.28 10:48 댓글 0

[의학신문·일간보사=김자연 기자] 미국에서 메드트로닉의 일부 인슐린 펌프가 사이버보안 위험 때문에 리콜을 당했다. FDA는 미니메드 508과 패러다임 시리즈에 대해 해킹당할 위험이 있다는 이유로 리콜했다.

FDA는 그 펌프들이 주변의 다른 기기와 커뮤니케이션하는 무선 프로토콜에 사이버보안의 구멍을 발견해 이용 환자는 그같은 위험으로부터 더욱 잘 보호되는 다른 모델로 교체해야 된다고 권고했다.

즉, 이들 펌프는 인근에 환자, 보호자, 의료진 말고도 누군가가 펌프에 무선으로 연결해 기기의 세팅을 바꿀 수 있다는 것.

그에 따라 인슐린이 과도하게 전달되면 환자는 저혈당으로 빠지고 인슐린 전달을 멈추면 고혈당 및 케톤산증을 겪게 된다.

덧붙여 FDA는 메드트로닉이 이들 펌프의 취약성에 관해 어떤 소프트웨어나 패치로도 적절하게 업데이트 시킬 수 없었다고 밝혔다.

통신 기능 없는 약물주입기...3000원짜리 적외선 레이저로 해킹

발행일 : 2016.08.07

'A대학병원 중환자실. 환자 옆에는 약액을 정확하게 투약하는 약물주입기가 놓여 있다. 회복되던 환자가 갑자기 알 수 없는 이유로 사망했다. 사인 규명을 위해 부검하니 약물 과다 투입이 원인이었다.' 우린 가끔 범죄 영화나 드라마에서 이 같은 허구 스토리를 접한다.

하지만 현실에서도 마음만 먹으면 이런 범죄가 매우 쉽게 자행될 수 있는 것으로 드러났다. 김용대 KAIST 전자공학과 시스템보안연구실 교수 연구팀은 인터넷에서 몇 천원이면 살 수 있는 적외선 레이저로 병원 중환자실에서 주로 쓰는 약물주입기(Infusion Pump) 센서의 해킹에 성공했다.

박영석 네이버랩스 연구원(KAIST 시스템보안연구실 석사 과정)이 주도한 관련 연구는 정보보호 학술지 '유즈닉스 우트(Usenix Woot)'의 논문에 채택됐다. 8월 9일 미국에서 열리는 공격기술 워크숍에서 발표된다.

<중환자실에 주로 쓰이는 약물주입기가 센서 스푸핑 공격으로 오작동을 유발하는 것으로 드러났다. ⓒ게티이미지뱅크>

의협 "원격의료 해킹에 무방비...보안 우려"

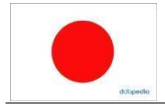
송고시간 | 2015-02-25 10:19

오수진 기자
기자 페이지

(서울=연합뉴스) 오수진 기자 = 현재 정부가 추진하는 원격의료 사업이 보안에 취약해 기술적 안전성에 큰 문제가 발생할 수 있다는 지적이 나왔다.

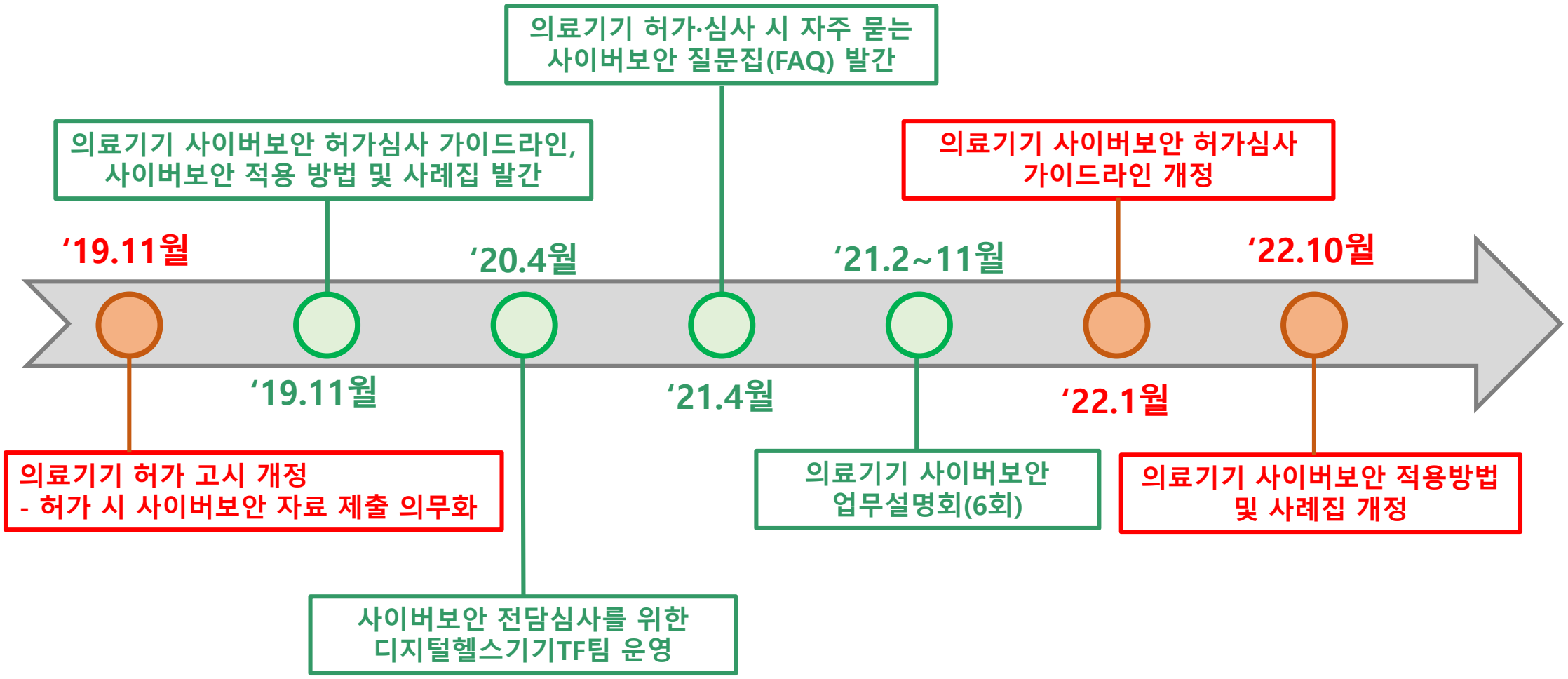
대한의사협회는 25일 오전 서울 용산구 의협회관에서 기자회견을 열고 "원격의료 서비스 운영에 대한 판단 근거와 안전성을 평가할 수 있는 기준을 제시하기 위해 연구 용역을 진행한 결과, 의료·헬스케어 분야가 금융 등 다른 산업보다 사이버 공격에 취약한 것으로 파악됐다"고 주장했다.

가이드라인 개발 배경 - 해외 규제 현황

국가	가이드라인 명
	- 의료기기의 사이버보안 허가·심사 가이드라인('22.1(개정)/'19.11) - 의료기기의 사이버보안 허가·심사 가이드라인('22.10(개정)/'19.11) - 의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ)('21.4)
	- 의료기기 사이버보안 품질관리 시스템 고려사항 및 시판 전 제출자료('22.4(개정)/'14.10) - 의료기기의 사이버보안 시판 후 관리('16.12)
	- 의료기기 사이버보안 보장 ('18.7)
	- 의료기기 사이버보안 가이드라인 (호주 TGA, '19.7)
	- 의료기기 사이버보안 시판 전 요구사항 (캐나다, '19.6)
	- 의료기기 사이버보안 가이드라인 (MDCG, '19.11)
IMDRF 국제의료기기 규제당국자포럼	- 의료기기 사이버보안 원칙 및 사례 (IMDRF, '20.1)

* IMDRF(International Medical Device Regulators Forum) : 미국, 유럽, 캐나다, 일본, 호주, 중국, 브라질, 러시아, 싱가포르, 대한민국 등 선진 10개국의 의료기기 규제당국자로 구성된 국제협의체

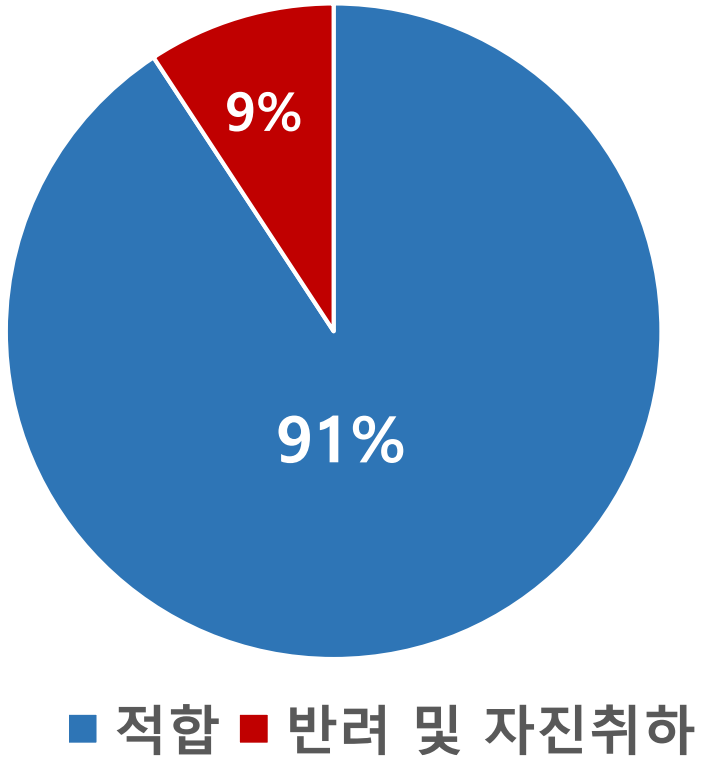
정책 추진 현황


의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ) 발간
의료기기 사이버보안 허가심사 가이드라인, 사이버보안 적용 방법 및 사례집 발간
의료기기 사이버보안 허가심사 가이드라인 개정
'19.11월
'20.4월
'21.2~11월
'22.10월
'19.11월
'21.4월
'22.1월
의료기기 허가 고시 개정
- 허가 시 사이버보안 자료 제출 의무화
의료기기 사이버보안 업무설명회(6회)
의료기기 사이버보안 적용방법 및 사례집 개정
사이버보안 전담심사를 위한 디지털헬스기기TF팀 운영
→ 디지털헬스규제지원과 신설('22.2월)

민원 처리 현황

➢ 가이드라인 개정 이후, **사이버보안 총 378건 처리(3,4등급)**

- **적합 : 343건(총 처리 민원 중 91%)**
- **자진취하 : 26건**
- **반려 : 9건**



조사 대상(허가 심사 대상 전체(인증 제외))

- 의료기기 기술문서(변경)심사/임상자료(변경)심사
- 의료기기 임상시험계획(변경)승인

조사 기간

- '22.1.21(가이드라인 개정)~'22.11월(현재)

허가·심사 방안 - 적용범위

별도로 내장된 펌웨어 없이 논리 연산 장치로 출력을 조절하는 레이저조사기

프로그램 가능 논리 제어기(PLC)를 포함하는 의료기기

사이버보안 적용 대상

소프트웨어(펌웨어)를 포함하는 의료기기

생체신호를 검출하고 경보를 발생하는 펌웨어가 내장된 환자감시장치

소프트웨어 의료기기 (SaMD)

스마트워치에서 측정된 혈압을 표시하는 모바일앱

소프트웨어를 포함하는 **통신 가능한 의료기기에 사이버보안 적용**

허가·심사 방안 - 요구사항

IMDRF 의료기기 사이버보안 설계 원칙

Design Principle	Description
Secure Communications 보안 통신	The manufacturer should consider how the device would interface with other devices or networks. Interfaces may include hardwired connections and/or wireless communications. Examples of interface methods include Wi-Fi, Ethernet, Bluetooth, USB, etc.
	The manufacturer should consider design features that validate all inputs (not just external) and take into account communication with devices and environments that only support less secure communication (e.g., a device connected to a home network or a legacy device).
	The manufacturer should consider how data transfer to and from the device is secured to prevent unauthorized access, modification, or replay. For example, manufacturers should determine: how the communications between devices/systems will authenticate each other; if encryption is required; how unauthorized replay of previously transmitted commands or data will be prevented; and if terminating communication sessions after a pre-defined time is appropriate.
Data Protection 데이터 보호	The manufacturer should consider if safety-related data that is stored on or transferred to/from the device requires some level of protection such as encryption. For example, passwords should be stored as cryptographically secure hashes.
	The manufacturer should consider if confidentiality risk control measures are required to protect message control/sequencing fields in communication protocols or to prevent the compromise of cryptographic keying materials.
Device Integrity 기기 무결성	The manufacturer should evaluate the system-level architecture to determine if design features are necessary to ensure data non-repudiation (e.g., supporting an audit logging function).
	The manufacturer should consider risks to the integrity of the device such as unauthorized modifications to the device software.
	The manufacturer should consider controls such as anti-malware to prevent viruses, spyware, ransomware, and other forms of malicious code of being executed on the device.
User Authentication 사용자 인증	The manufacturer should consider user access controls that validate who can use the device or allows granting of privileges to different user roles or allow users access in an emergency. Additionally, the same credentials should not be shared across devices and customers. Examples of authentication or access authorization include passwords, hardware keys, or biometrics, or a signal of intent that cannot be produced by another device.
Software Maintenance 소프트웨어 유지보수	The manufacturer should establish and communicate a process for implementation and deployment of regular updates.
	The manufacturer should consider how operating system software, third-party software, or open source software will be updated or controlled. The manufacturer should also plan how to respond to software updates or outdated operating environments outside of their control (e.g. medical device software running on an unsecure operating system version).
	The manufacturer should consider how the device will be updated to secure it against newly discovered cybersecurity vulnerabilities. For example, consideration could be given to whether updates will require user intervention or be initiated by the device and how the update can be validated to ensure it has no adverse effect on the safety and performance of the device.
	The manufacturer should consider what connections will be required to conduct updates and the authenticity of the connection or update through the use of code signing or other similar methods.
Physical Access 물리적 접근	The manufacturer should consider controls to prevent an unauthorized person from accessing the device. For example, controls could include physical locks or physically restricting access to ports, or not allowing access with a physical cable without requiring authentication.
Reliability and Availability 신뢰성 및 가용성	The manufacturer should consider design features that will allow the device to detect, resist, respond and recover from cybersecurity attacks in order to maintain its essential performance.

Principles and Practices for Medical Device Cybersecurity, IMDRF(2020)

허가·심사 방안 - 요구사항

국내 의료기기 사이버보안 요구사항

항목	요구사항
보안 통신	제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등
	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.
	제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송·수신 방법을 고려하여야 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
데이터 보호	제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송·수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보안(secure)이 확보된 해쉬(hash)로 저장되어야함
	제조자는 기밀성에 대한 위험 통제 수단이 요구될 때, 통신 프로토콜의 컨트롤(control)/시퀀싱(sequencing) 필드의 메시지를 보호하거나 암호화의 키 관련 자료가 손상되는 것을 방지하도록 고려하여야 한다.
기기 무결성	제조자는 데이터 부인방지(non-repudiation)를 보장하기 위한 설계 특성이 필요한지를 결정하기 위해 시스템 레벨에서의 아키텍처를 평가하여야 한다. ※ 예: 감사 로그 기록 기능 제공
	제조자는 기기 소프트웨어의 비인가된 변경과 같은 기기의 무결성에 대한 위험을 고려해야한다.
	제조자는 바이러스, 스파이웨어, 랜섬웨어 등 기기에서 실행될 수 있는 악성코드를 막기 위해 안티 멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.
사용자 인증	제조자는 기기의 사용이 인증된 사용자이거나, 다른 역할의 사용자에게 사용권한을 부여를 허용하거나, 응급상황에서 접근을 허용하는 사용자 접근 통제에 대해 고려하여야 한다. 추가적으로 동일한 자격증명은 기기와 고객들에게 공유되지 않아야한다. ※ 접근 통제의 예: 비밀번호, 하드웨어 키, 생체인증 등
소프트웨어 유지보수	제조자는 주기적인 업데이트의 구현과 배포를 위한 수행절차를 수립하고 통보하여야한다.
	제조자는 운영 체제(OS) 소프트웨어, 제3자 소프트웨어, 오픈 소스 소프트웨어가 업데이트나 통제될 경우에 대해 고려하여야 한다. 또한 제조자는 외부의 통제에 의한 소프트웨어의 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.
물리적 접근	제조자는 비인가된 개인이 의료기기에 접근하는 것을 방지하기 위한 통제수단을 고려하여야 한다. ※ 예: 물리적 잠금 혹은 포트(port) 접근의 물리적 제한, 인증이 필요없는 물리적 케이블의 접근제한 등
신뢰성 및 가용성	제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.

허가·심사 방안 - 제출자료

< 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

제출자료를 검토하여 **제품의 사이버보안 안전성을 확인**

허가·심사 방안 - 제출자료

< 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 요구사항에 대한 적합성 여부**를 확인할 수 있는 자료
- 의료기기 사이버 보안 **필수원칙 체크리스트 양식을 활용하여 제품의 특성에 맞게 작성**

허가·심사 방안 - 제출자료

< 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 위험관리 과정에서 식별된 위해요인에 대한 **위험통제 조치의 결과를 검증할 수 있는 객관적인 자료**
- 의료기기 전체 생명주기에서의 사이버보안과 관련된 위해요인을 파악하여 **발생 가능한 위해를 최소화 및 차단하기 위한 위험관리 활동**을 기록

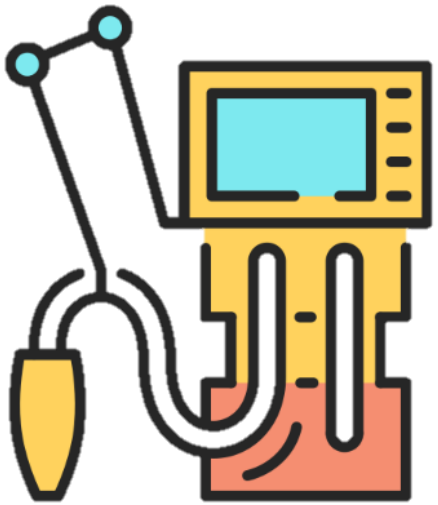
허가·심사 방안 - 제출자료

< 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

- 특정 요구사항을 미적용하더라도 **사이버보안 침해로 인해 환자에게 미치는 위험이 허용가능한 수준임을 확인**할 수 있는 자료

허가·심사 방안 – 심사 사례



무선 랜(Wi-Fi)

환자 생체정보 송수신

업데이트 수행

의료기기

제조원 서버

<공용 네트워크망 접속 의료기기 통신 구성도>

허가·심사 방안 – 심사 사례

사이버보안 요구사항	해당기기 적용여부	적합성 입증 방법	해당 첨부자료 또는 문서번호	적합성 입증 방법
보안 통신				
제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등	적용	사용설명서, 기술문서 (모양 및 구조- 특성)	-	- 제품의 통신 구성 및 방법을 확인할 수 있는 통신구성도, 사용설명서 제출
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.	적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (3.4.1 보안 통신)	- 제품은 제조사의 서버 주소로만 접속이 가능하며 이 외에는 무선랜을 통한 접근이 불가함. - 제조사 서버와 연결 후 5분간 활동이 없을 경우 연결이 자동으로 종료됨.
제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송·수신 방법을 고려하여야 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	적용			

허가·심사 방안 – 심사 사례

사이버보안 요구사항	해당기기 적용여부	적합성 입증 방법	해당 첨부자료 또는 문서번호	적합성 입증 방법
데이터 보호				
제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송·수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보안(secure)이 확보된 해쉬(hash)로 저장되어야함	적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (4.3.1 데이터 암호화)	- TLS 1.2 프로토콜이 적용되어 암호화된 안전한 HTTPS 네트워크망을 사용하여야만 데이터가 전송되며, HTTP로는 데이터 전송이 불가함.
제조자는 기밀성에 대한 위험 통제 수단이 요구될 때, 통신 프로토콜의 컨트롤(control)/시퀀싱(sequencing) 필드의 메시지를 보호하거나 암호화의 키 관련 자료가 손상되는 것을 방지하도록 고려하여야 한다.	적용			

허가·심사 방안 – 심사 사례

사이버보안 요구사항	해당기기 적용여부	적합성 입증 방법	해당 첨부자료 또는 문서번호	적합성 입증 방법
기기 무결성				
제조자는 데이터 부인방지(non-repudiation)를 보장하기 위한 설계 특성이 필요한지를 결정하기 위해 시스템 레벨에서의 아키텍쳐를 평가하여야 한다. ※ 예: 감사 로그 기록 기능 제공	적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (5.1 시스템 로그 기록)	- 데이터 송수신 정보, 업데이트 이력, 변경/삭제 로그가 서버에 기록됨
제조자는 기기 소프트웨어의 비인가된 변경과 같은 기기의 무결성에 대한 위험을 고려해야한다.	적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (4.9 실행파일 무결성 검증)	- 제품 구동 시, 기기 내의 주요 실행파일 및 DLL 들의 버전정보를 확인하고 실행파일에 인증서가 포함되었는지 여부를 확인함. - 체크섬을 이용하여 서버와 기기 간 패킷의 무결성을 검증함
제조자는 바이러스, 스파이웨어, 랜섬웨어 등 기기에서 실행될 수 있는 악성코드를 막기 위해 안티 멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.	적용			

허가·심사 방안 – 심사 사례

사이버보안 요구사항	해당기기 적용여부	적합성 입증 방법	해당 첨부자료 또는 문서번호	적합성 입증 방법
사용자 인증				
제조자는 기기의 사용이 입증된 사용자이거나, 다른 역할의 사용자에게 사용권한을 부여를 허용하거나, 응급상황에서 접근을 허용하는 사용자 접근 통제에 대해 고려하여야 한다. 추가적으로 동일한 자격증명은 기기와 고객들에게 공유되지 않아야한다. ※ 접근 통제의 예: 비밀번호, 하드웨어 키, 생체인증 등	적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (3.4.1 보안 통신)	- 제품은 제조사의 서버 주소로만 접속이 가능하며 이 외에는 무선랜을 통한 접근이 불가함. - 제조사 서버와 연결 후 5분간 활동이 없을 경우 연결이 자동으로 종료됨.

허가·심사 방안 – 심사 사례

사이버보안 요구사항	해당기기 적용여부	적합성 입증 방법	해당 첨부자료 또는 문서번호	적합성 입증 방법
소프트웨어 유지보수				
제조자는 주기적인 업데이트의 구현과 배포를 위한 수행절차를 수립하고 통보하여야한다.	적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (4.2 소프트웨어 업데이트 인증 방식 사용)	- 소프트웨어 유지보수 지침서 에 따라 펌웨어 및 소프트웨어 업데이트 시 연구개발팀장 및 품질책임자가 소프트웨어 변경 요청 및 승인하는 절차가 있음을 확인 - 업데이트 파일은 인증된 제조사 서버에 접속하여야만 수신이 가능함. - CRC 체크를 통해 업데이트 파일의 무결성을 검증함
제조자는 운영 체제(OS) 소프트웨어, 제3자 소프트웨어, 오픈 소스 소프트웨어가 업데이트나 통제될 경우에 대해 고려하여야 한다. 또한 제조자는 외부의 통제에 의한 소프트웨어의 업데이트나 운영환경 만료에 대한 대응 계획을 수립하여야 한다. ※ 예: 보안이 보장되지 않은(unsecure) 운영체제 버전에서 운영되는 의료기기 소프트웨어	적용			
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	적용			
제조자는 업데이트를 수행하기 위해 어떤 연결이 필요한지와 코드 서명 및 기타 비슷한 수단을 통한 연결이나 업데이트의 진본성을 고려하여야 한다.	적용			

허가·심사 방안 – 심사 사례

사이버보안 요구사항	해당기기 적용여부	적합성 입증 방법	해당 첨부자료 또는 문서번호	적합성 입증 방법
물리적 접근				
제조자는 비인가된 개인이 의료기기에 접근하는 것을 방지하기 위한 통제수단을 고려하여야 한다. ※ 예: 물리적 잠금 혹은 포트(port) 접근의 물리적 제한, 인증이 필요없는 물리적 케이블의 접근제한 등	미적용	-	-	**[미적용 사유]** - 신청제품은 무선 랜 통신(Wi-Fi)을 사용하여, 접근가능한 물리적 통신포트가 없음.
신뢰성 및 가용성				
제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.	적용	사용설명서	AISW_IFU_ver2.0 (7.1 기기 고장 시 대응 방안)	- 사용설명서를 통해 의료기기 사용 중 발생하는 사이버보안 사고 시 연락할 수 있는 긴급 연락처 및 사이버보안 위협 탐지 시에 취해야할 대응책을 제공함.

주요 보완 사례

- 사이버보안 체크리스트, 첨부자료 미제출
- 개정 이전의 사이버보안 체크리스트 제출
- 소프트웨어 적합성 확인보고서에 통신 목적 미기재
- '모양 및 구조-특성' 에 사이버보안 특성 및 통신구성도 미기재
- 사용 시 주의사항에 사이버보안 위협 탐지 시 취해야할 대응책 미기재

주요 보완 사례

● **사이버보안 체크리스트 및 첨부자료 미제출**

< 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

주요 보완 사례

● 개정 이전의 사이버보안 체크리스트 제출

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.				
1.3 사용자(의료기기) 접속 인식 비인가된 사용자(의료기기)가 접속될 시 이를 인식하여 구분할 수 있어야 한다.				
1.4 비인가된 사용자(의료기기) 접속 제한 비인가된 사용자(의료기기)의 접속 시 접속을 제한할 수 있어야 한다.				
1.5 비인가된 네트워크 통신 차단 비인가된 네트워크 통신 접속을 제한할 수 있어야 한다.				
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.				

'19.11월 발간된 체크리스트

사이버보안 요구사항		해당 기기 적용 여부	적합성 입증 방법	해당 첨부자료 또는 문서번호
보안 통신	제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등	*적용/미적용*	*소프트웨어 검증 및 유효성 확인 자료/사이버보안 위험관리문서*	*문서번호, 페이지, 요구사항 ID, 시험항목 #*
	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.			
	제조자는 비인가 접근/변경/반복을 방지하기 위한 의료기기의 보안이 보장된(secured) 데이터 송·수신 방법을 고려하여야 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			
데이터 보호	제조자는 안전(safety)과 관련된 데이터가 저장되거나 기기와 송·수신될 때 암호화와 같은 일정 수준의 보호가 요구되는지 고려하여야 한다. ※ 예: 비밀번호(passwords)는 암호화된 보			

별첨 의료기기 사이버보안 요구사항 예시

표 2의 의료기기 사이버보안 요구사항에 적용할 수 있는 상세한 예시를 아래에 제시하였으며 제조자는 상세 예시를 참고하여 각 요구사항에 대한 적합성을 입증할 수 있다. 다만, 해당 예시는 참고 사항일 뿐이며 반드시 이를 따를 필요는 없다.

[표 5. 사이버보안 요구사항에 대한 상세 요구사항 예시]

항목	사이버보안 요구사항	상세 요구사항 예시	
보안 통신	제조자는 의료기기가 다른 기기나 네트워크와 어떻게 접속(유·무선 통신 등)하여야할지를 고려하여야 한다. ※ 예: Wi-Fi, 이더넷, 블루투스, USB 등	[1] 통신 구성 제품의 위해도 및 사용환경을 고려하여 통신을 구성하여야한다. ※ 입증 예시 : 제품의 통신 구성 및 방법을 확인할 수 있는 통신구성도, 사용설명서 등	
	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 따라 인가된 데이터에만 접근 가능해야 한다.	[2-1] 통신 시 인가된 기기 또는 네트워크를 인식할 수 있는 수단을 갖추어야한다.
			[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.

'22.1월 개정

주요 보완 사례

● 소프트웨어 적합성 확인보고서에 통신 목적 기재 필요

[별표 13]

의료기기 소프트웨어 적합성 확인보고서 작성방법(제29조제4호 관련)

1. 품목명

「의료기기 품목 및 품목별 등급에 관한 규정」(식품의약품안전처 고시)에 따라 소프트웨어가 사용되는 의료기기의 품목명, 분류번호 및 등급을 작성한다.

2. 소프트웨어 명칭 및 버전

소프트웨어의 명칭 및 버전을 작성한다.

3. 소프트웨어 사용형태

의료기기 소프트웨어 사용형태에 따라 내장형, 독립형으로 구분하여 표시한다.

4. 소프트웨어 기능적 특성

의료기기 소프트웨어의 해당되는 기능적 특성에 따라 표시한다.

5. 소프트웨어 안전성 등급

의료기기 소프트웨어 안전성 등급은 소프트웨어의 고장, 설계 결함 또는 사용 시 발생할 수 있는 잠재적 결함으로부터 환자, 사용자 또는 기타 사람에게 영향을 끼칠 수 있는 위해의 정도에 따라 아래 표와 같이 A등급, B등급, C등급으로 구분할 수 있으며, 적합성 확인보고서에는 해당 소프트웨어의 안전성 등급 및 안전성 등급 판단에 대한 제조사의 해당 문서 관리번호를 기재한다.

등급	의료기기 소프트웨어 안전성 등급 정의
A 등급	부상이나 신체적 피해가 발생할 가능성이 없음
B 등급	심각하지 않은 부상(경상)이 발생할 가능성이 있음
C 등급	심각한 부상 또는 사망이 발생할 가능성이 있음

6. 소프트웨어의 사용목적

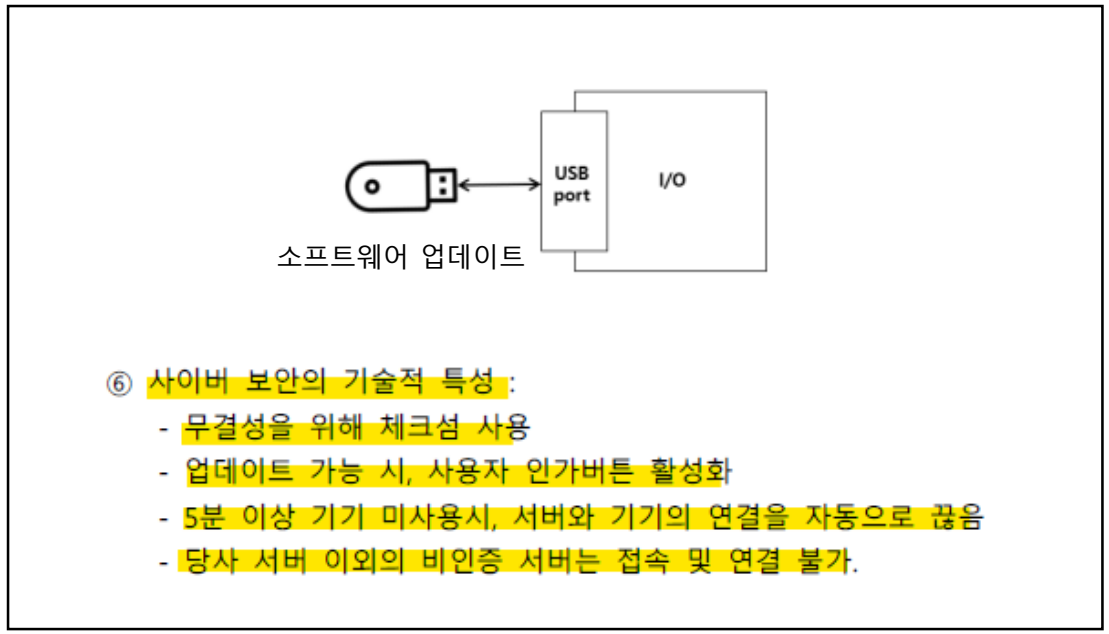
해당 의료기기의 통신 기능이 있는 경우, 통신 목적(제어, 모니터링, 유지보수 및 통신표준 등)을 포함하여 소프트웨어의 사용목적을 작성한다.

의료기기 소프트웨어 적합성 확인보고서

품목명 (품목분류번호)		소프트웨어 명칭 및 버전	
소프트웨어 사용형태	[O] 내장형	[ ] 독립형	
소프트웨어 기능적 특성 (중복선택 가능)	[O] 제어 [ ] 진단 [ ] 데이터 수신	[O] 측정 [ ] 데이터 변환 [O] 표시	[O] 분석 [O] 데이터 전송 [ ] 기타
소프트웨어 안전성 등급	[ ] A	[O] B	[ ] C
소프트웨어 사용목적	[redacted]의 약물주입을 위한 모터제어, 화면 표시, 사운드 제어, 알람규격에 맞는 LED제어 등을 담당한다. 무선 지그비 통신을 통해 [redacted] 유속 주입량, 기기 상태를 [redacted] 전송한다.		
소프트웨어 운영환경 (독립형 소프트웨어에 한함)	Target : STM32L151RE/STM32L151CB Compiler : Eclips Tool: ST-Link V2 DownLoader: ST-Utility		

주요 보완 사례

● **허가증 내 사이버보안 기술적 특성 기재 필요**

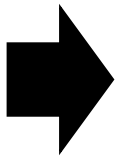


'모양 및 구조-특성' 작동계통도(통신구성도)에 **제품의 통신 구성과 사이버보안 기술적 특성을 기재**

주요 보완 사례

● 사용 시 주의사항에 사이버보안 위협 탐지 시 취해야할 대응책 기재

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.
신뢰성 및 가용성	제조자는 의료기기가 필수 성능을 유지하기 위해 사이버보안 공격을 탐지, 저항, 대응 및 복구하도록 허용하는 설계 특성을 고려하여야 한다.



4. 일반적 주의

- 당사의 기술자 또는 당사로부터 위임을 받은 기술자만이 기기를 열 수 있습니다.
- 사용자가 기기를 열거나 기기의 부품을 바꾸려고 하는 행위는 엄격히 금지되어 있습니다.
- 이 기기는 숙달된 전문가의 감독 하에서만 사용되어야 합니다.
- 전원 플러그를 제거하기 어려운 곳에 기계를 설치하지 마십시오.
- 이 기기를 액체류 가까이에 두지 마십시오.
- 전자기 간섭을 일으킬 수 있는 기기 근처에서 이 기기를 사용할 때 주의를 기울여야 합니다. 시술 시 전자기 간섭을 최소화하기 위해 다른 기기를 멀리하십시오.
- 감전되지 않도록 시스템의 유지관리 절차를 진행하기 전에 전원 공급 장치(전기 콘센트)에서 장치를 분리해야 한다.
- 힘으로 전기 코드나 부속품을 구부리지 말고, 항상 쉽게 접근할 수 있도록 하십시오.
- 기기와 액세서리가 정상적으로 작동하는지의 여부를 정기적(최소 2년)으로 확인하십시오.
- 기기와 액세서리는 물, 젤, 크림, 기름 등의 침습에 취약합니다. 침수, 침습은 기기 고장 및 환자 부상의 원인이 될 수 있습니다
- 어린아이의 손에 미치지 않는 곳에 보관하여야 한다.
- 이 기기는 리튬 이온 배터리를 사용합니다. 이 기기를 가방에 넣고 비행기를 타지 마십시오.
- 사이버 보안 위협 탐지 시 먼저 와이파이 연결을 끊고 기기의 전원을 종료하십시오. 이후 당사의 연락처[redacted]로 연락하여 조치를 취하십시오

➢ 사이버보안 대응책을 **사용설명서 및 ' 사용 시 주의사항'에 기재**

국민 안심이 기준입니다

YOUR SAFETY IS OUR STANDARD

식품의약품안전처