의료기기 사이버보안 업무설명회(11차)

2023. 3. 15.

국민권익위원회가 함께하는 청렴韓세상

식품의약품안전처 식품의약품안전평가원

더 건강한 국민의 내일을 위한 정부혁신 보다나은 식약처+

식품의약품안전처

목 차

식품의약품안전처

Ⅰ. 설명회 운영계획

‘22년도 사이버보안 업무설명회 운영 계획

❍ **(일시 및 장소)** ‘23.3월, 7월, 11월, 온라인(1시간 30분), 총 3회

❍ **(대 상)** 의료기기 제조·수입 업체 인허가 담당자 및 개발자

* 원활한 접속 및 운영 등을 위해 사전등록은 선착순으로 1000명 제한

❍ **(주요 내용)**

- 사이버보안 규제 현황(가이드라인 도입 배경 및 주요 내용) 설명
- 제품 형태(HW/SW/HW+SW) 별 구체적인 심사 사례, 제출 자료 및 주요 보완 사례 제시
- 허가·인증 변경 시, 사이버보안 제출 자료 및 허가증 기재 방안

‘22년도 사이버보안 업무설명회 운영 계획

❍ **(설명회 평가)** 설명회 종료 후 업무설명회 평가 및 개선 의견 등 설문조사

❍ **(발표자료)** 설명회 종료 후, 식약처 홈페이지에 발표자료 게시 예정

* 식약처 홈페이지 → 법령/자료 → 자료실 → 학술 토론회

‘22년도 사이버보안 업무설명회 운영 계획

❍ **세부 프로그램**

<table>
<tr><th>시간(총 90분)</th><th>일 정</th><th>비 고</th></tr>
<tr><td>5 ‘</td><td>인사말</td><td></td></tr>
<tr><td>15 ‘</td><td>의료기기 사이버보안 규제 현황
(가이드라인 도입 배경 및 주요 내용)</td><td></td></tr>
<tr><td>30 ‘</td><td>제품 형태 별 사이버보안 자료 제출, 심사 사례,
주요 보완 사례
<table><tr><th>일정</th><th>사이버보안 심사 사례 발표 주제</th></tr><tr><td>3월</td><td>전기사용 의료기기(하드웨어/HW)</td></tr><tr><td>7월</td><td>독립형 소프트웨어(소프트웨어/SW)</td></tr><tr><td>11월</td><td>장치(하드웨어) + 모바일앱(소프트웨어) 조합</td></tr></table></td><td></td></tr>
<tr><td>10 ‘</td><td>자주 묻는 질의 및 답변 공유</td><td></td></tr>
<tr><td>30 ‘</td><td>질의 응답</td><td></td></tr>
</table>

식품의약품안전처

Ⅱ. 의료기기 사이버보안 규제 현황

가이드라인 개발 배경

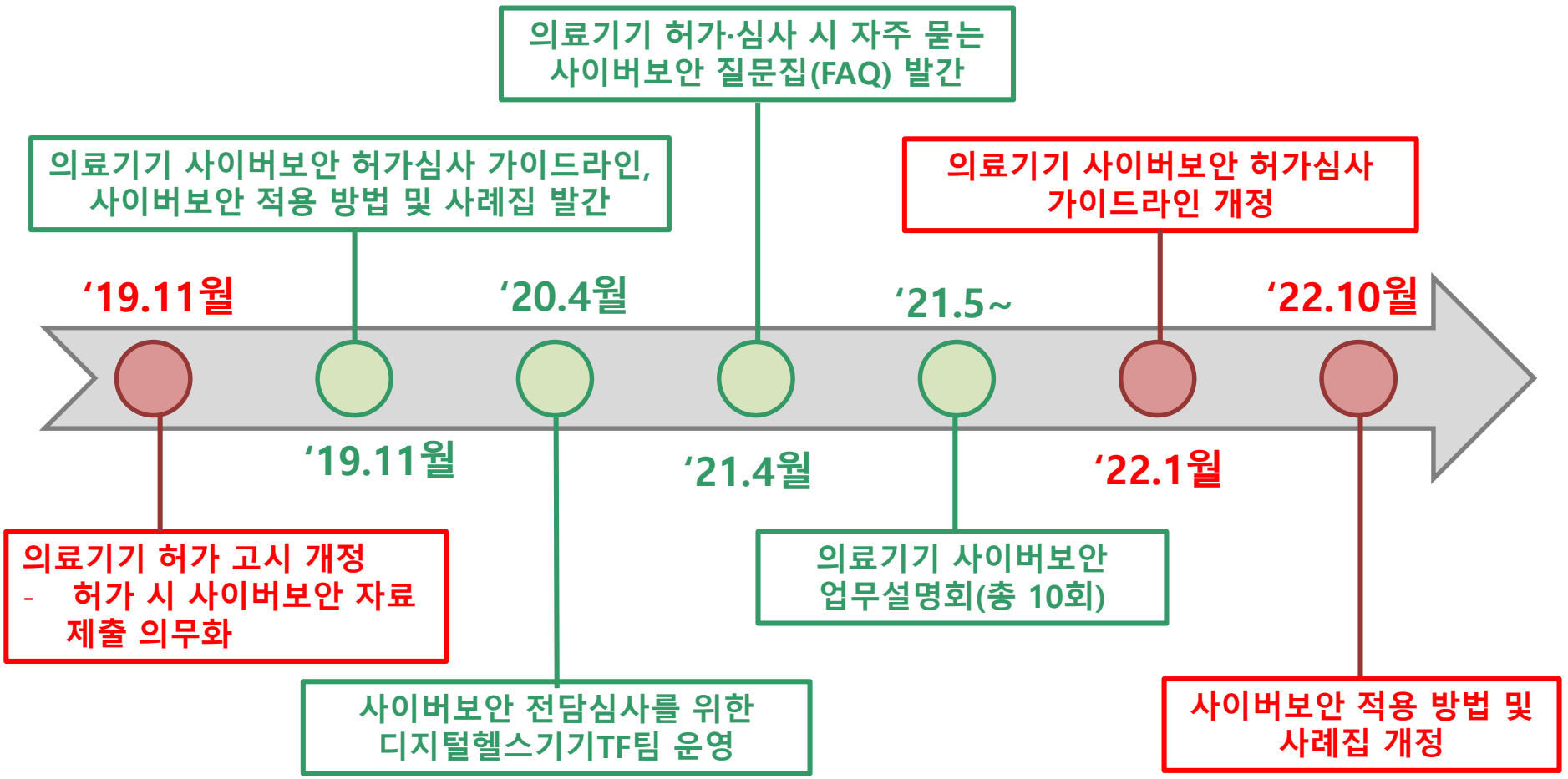
- 모바일 앱을 이용하여 개인의료정보, 생체신호 송수신, 기기 제어 등 수행

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

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

- 유무선 통신을 이용하여 수술용 기기를 제어

정책 추친 현황



→ 디지털헬스규제지원과 신설('22.2월)

허가심사 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**

허가심사 방안 – 기본 원칙

제조자는 의료기기의 사이버 보안을 보장하기 위하여

기밀성, 무결성, 가용성의 3대 원칙 준수 요구

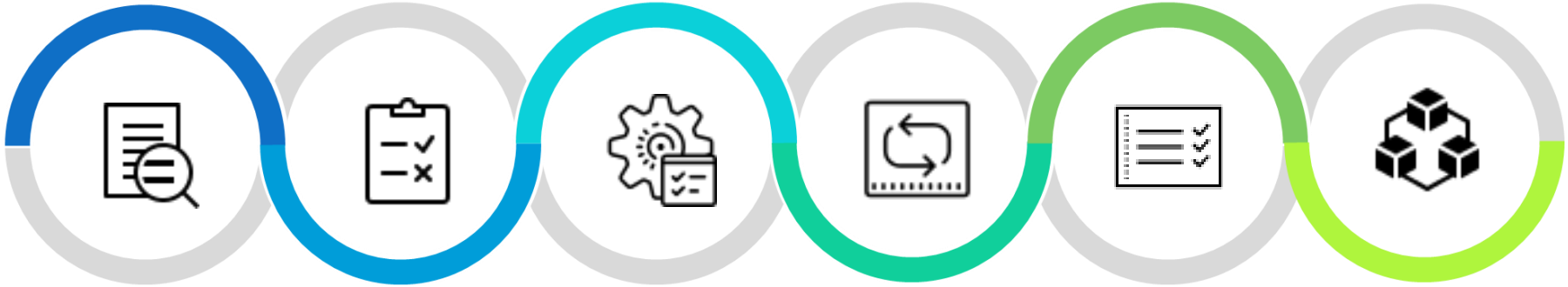
개인의료정보가 허가되지 않은 사람에게 공개되거나, 허가되지 않은 용도로 사용되지 않게 하는 기능

개인의료정보가 허가되지 않은 방법으로 변환되거나 파괴되지 않도록 하는 기능

개인의료정보가 승인된 사용자에게는 즉시 제공되어야 하며, 필요한 때에 필요한 곳에서 필요한 형태로 존재하도록 하는 기능

허가심사 방안 - 원칙

의료기기 제조품질관리체계의 **위험관리 프로세스를 통해 사이버보안 적용**



위험분석	위험평가	위험통제	잔여위험 허용평가	위험관리 보고서	생산 및 생산 후 정보
기밀성, 가용성, 무결성이 파괴되어 환자에게 미치는 위해요인 식별	산정된 위험이 위험감소를 하지 않아도 될 만큼 낮은지 결정	적절한 사이버 보안 위험통제 방안의 선택 및 실행	위험통제 수단의 적용 후 잔여위험들에 대한 허용평가 수행	사이버 보안 위험관리 프로세스에서의 절차들을 위험관리 보고서에 기록	사이버 보안에 대한 정보를 검토하기 위한 체계적인 절차 수립 및 유지

허가심사 방안 - 요구사항

IMDRF 의료기기 사이버보안 설계 원칙

Design Principle	Description
보안 통신 Secure Communications	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.
데이터 보호 Data Protection	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.
기기 무결성 Device Integrity	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.
사용자 인증 User Authentication	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.
소프트웨어 유지보수 Software Maintenance	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.
물리적 접근 Physical Access	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	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.

신뢰성 및 가용성

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

허가심사 방안 - 요구사항

요구사항 적용 시 고려사항

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

허가심사 방안 - 요구사항

의료기기 사이버보안 필수원칙 체크리스트

< 의료기기 사이버보안 특성 기재 >

1) 사용되는 통신 기술 : *유선 통신(USB, RS-232, LAN), 무선 통신(Wi-Fi, 블루투스, RF 통신)*

2) 사용환경 : *병원 내 사용, 병원 외 사용*

3) 공용 네트워크망 사용여부 : *Y/N*

사이버보안 요구사항		해당 기기 적용 여부	적합성 입증 방법	해당 첨부자료 또는 문서번호
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			

허가심사 방안 – 제출 자료

< 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**

허가심사 방안 – 제출 자료

< 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**

허가심사 방안 – 제출 자료

< 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

허가심사 방안 – 제출 자료

< 사이버보안 제출 자료 예시 >

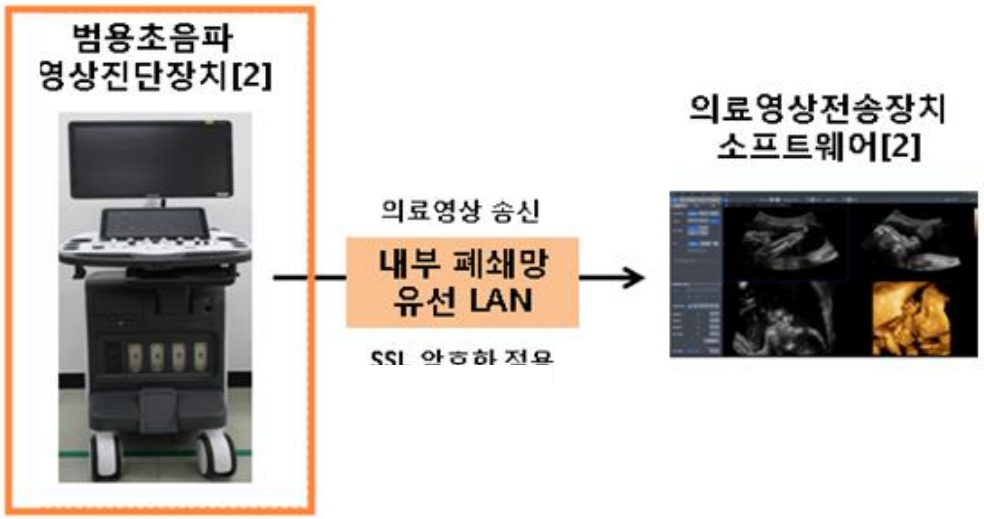
1. 의료기기 사이버보안 요구사항 체크리스트
2. 사이버보안 요구사항을 검증한 자료
   - 소프트웨어 검증 및 유효성 확인 자료
   - 사이버보안 위험관리문서
   - 성능시험성적서
3. 사이버보안 요구사항 미적용 근거를 확인할 수 있는 자료
   - 사이버보안 위험관리문서 등

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

식품의약품안전처

Ⅲ. 사이버보안 자료 제출, 심사 사례, 주요 보완 사례

사이버보안 요구사항 체크리스트 심사 사례



- 통신방법 : LAN 통신
- 사용환경 : 병원 내 사용
- 공용 네트워크망 사용 여부 : N

사이버보안 요구사항 체크리스트 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, 사용설명서	VVT-SW-001 (3.4.1 접근 통제 및 인증), AISW_IFU_ ver2.0 (5.3 사용 시 주의사항)	- 제품은 병원 폐쇄망 내에서 사용되어 **방화벽을 통해 비인가 포트로의 접근이 불가**함. - 사용자 매뉴얼 및사용 시 주의사항에 본 제품은 물리적으로 망이 분리된 폐쇄망 내에서만 사용하여야함을 확인함.
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			

사이버보안 요구사항 체크리스트 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)	- DICOM 영상은 HTTP에 **TLS 1.2 프로토콜이 적용**되어 암호화된 안전한 HTTPS 네트워크망을 사용하여야만 데이터가 전송됨. HTTP로는 전송 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	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (4.3.2 암호키 저장)	- 암호화 시에 사용되는 **암호키는** 데이터가 저장되는 데이터베이스와 **분리된 장소에 저장**됨.

사이버보안 요구사항 체크리스트 심사 사례

데이터 암호화 미적용 입증 방법

1. 근거자료(위험관리문서 등) 제출

- 병원 폐쇄망 내에서 사용되는 제품으로, 개인의료정보를 암호화하지 않더라도 정보의 위변조로 인한 위험이 허용할만한 수준임을 확인할 수 있는 위험관리 문서 등을 제출

2. '사용 시 주의사항' 에 사용환경을 명시

- (예시) 해당 소프트웨어는 데이터에 대한 암호화 통신을 하지 않는 제품으로 병원의 폐쇄망에서만 사용되어야 하며, 방화벽이나 백신 등 보안시스템이 갖춰진 PC를 사용할 것

사이버보안 요구사항 체크리스트 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)	- **환자 생체신호 송수신 정보, 변경/삭제 로그가 기록**되며, 관리자 계정으로 접속 시 시스템 로그 기록을 열람할 수 있음.
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 버전 정보를 확인하고 **실행파일에 인증서가 포함되었는지 여부를 확인**함.
제조자는 바이러스, 스파이웨어, 랜섬웨어 등 기기에서 실행될 수 있는 악성코드를 막기 위해 안티 멀웨어 프로그램과 같은 통제조치를 고려하여야 한다.	적용			

사이버보안 요구사항 체크리스트 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 접근 통제 및 인증)	- 제품은 병원 폐쇄망 내에서 사용되어 **방화벽을 통해 비인가 포트로의 접근이 불가**함.

사이버보안 요구사항 체크리스트 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 절차**가 있음을 확인 - **업데이트 파일의 디지털 서명을 확인하여 무결성 검증** 후 업데이트 파일이 실행됨. - 업데이트 파일 **실행 전 버전을 식별**하여 낮은 버전의 업데이트는 수행되지 않음.
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			

사이버보안 요구사항 체크리스트 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.	미적용	소프트웨어 검증 및 유효성 확인 자료	VVT-SW-001 (4.2 소프트웨어 업데이트 인증 방식 사용)	**[미적용 사유]** - 본 제품은 서비스 엔지니어가 메인보드에 직접 접속하여야만 업데이트가 가능하며, LAN 포트를 통해 수신된 소프트웨어 업데이트 파일은 실행 불가함.
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 업데이트를 수행하기 위해 어떤 연결이 필요한지와 코드 서명 및 기타 비슷한 수단을 통한 연결이나 업데이트의 진본성을 고려하여야 한다.				

사이버보안 요구사항 체크리스트 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 물리적 포트를 사용하는 제품으로 해당 항목에 대한 안전성 입증이 불가함 - 따라서, 물리적 잠금장치가 아닌 소프트웨어적 통제 조치(사용자 계정을 통한 접근통제, 암호화 알고리즘 등)를 이용하여 사이버보안 안전성을 입증하였음
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 제공**함

사이버보안 관련 주요 보완 사례

- 사이버보안 체크리스트, 첨부자료 미제출
- 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

사이버보안 관련 주요 보완 사례

● **사이버보안 체크리스트 및 첨부자료 제출 필요**

< 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

사이버보안 관련 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

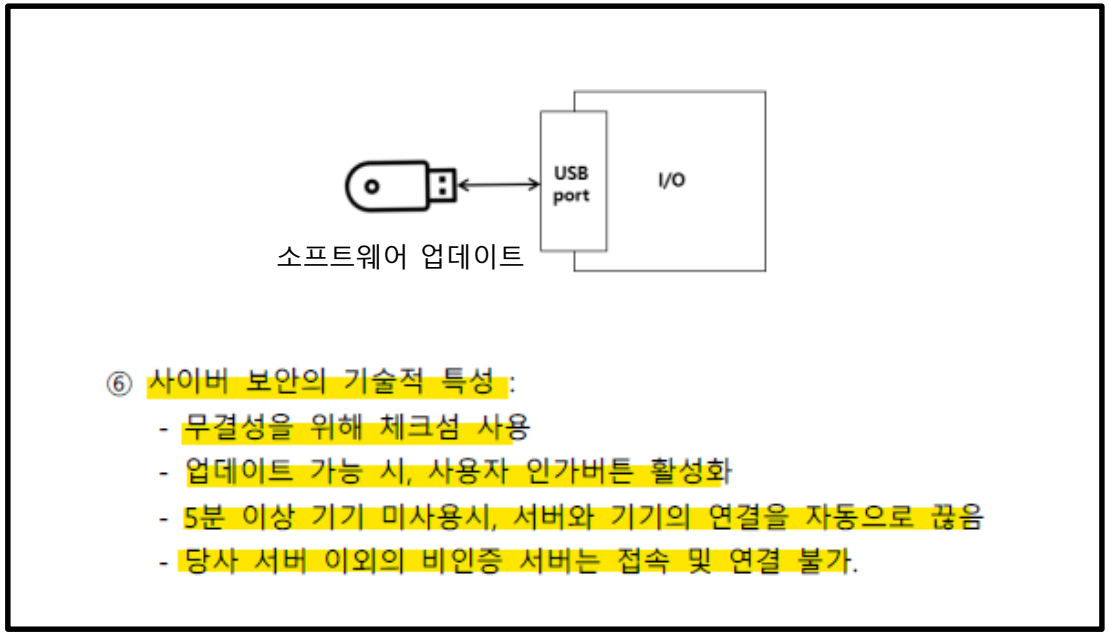
6. 소프트웨어의 사용목적
해당 의료기기의 통신 기능이 있는 경우, 통신 목적(제어, 모니터링, 유지보수 및 통신표준 등)을 포함하여 소프트웨어의 사용목적을 작성한다.

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	의 약물주입을 위한 모터제어, 화면 표시, 사운드 제어, 알람규격에 맞는 LED제어 등을 담당한다. 무선 지그비 통신을 통해 유속 주입량, 기기 상태를 전송한다.		
소프트웨어 운영환경 (독립형 소프트웨어에 한함)	Target : STM32L151RE/STM32L151CB Compiler : Eclips Tool: ST-Link V2 DownLoader: ST-Utility		

사이버보안 관련 주요 보완 사례

● **허가증 내 사이버보안 기술적 특성 기재 필요**



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

사이버보안 관련 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.

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 로 연락하여 조치를 취하십시오

- 사이버보안 대응책을 **사용설명서 및 ' 사용 시 주의사항'에 기재**
- 임상시험계획승인 시에는 계획서 내의 **'예측되는 부작용 및 사용 시 주의사항 ' 에 기재**

식품의약품안전처

Ⅳ. 허가·인증 변경 시, 사이버보안 관련 제출 자료 및 허가신청서 기재 방안

의료기기 변경 허가 시 제출자료 등 개선 방안

● **현황**

사이버보안 제출자료

- 사이버보안 요구사항 체크리스트
- 소프트웨어 검증 및 유효성 확인 자료

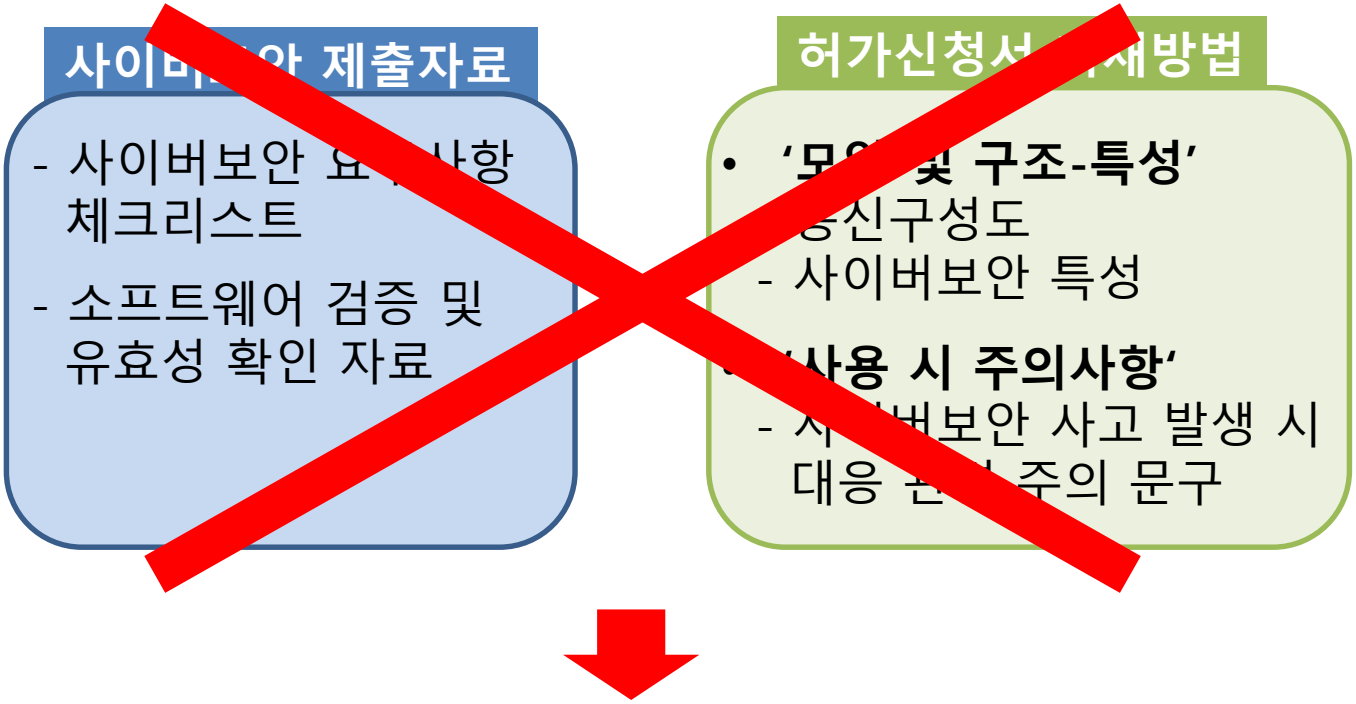
허가신청서 기재방법

- **'모양 및 구조-특성'**
  - 통신구성도
  - 사이버보안 특성
- **'사용 시 주의사항'**
  - 사이버보안 사고 발생 시 대응 관련 주의 문구

현재는 사이버보안 제출자료를 근거로 허가신청서에 관련 사항을 기재

의료기기 변경 허가 시 제출자료 등 개선 방안

● 문제점



사이버보안 자료 의무 제출 제도('19.11월) 시행 이전에 허가 받은 제품에는 제출자료 및 허가신청서 기재가 반영되지 않음

의료기기 변경 허가 시 제출자료 등 개선 방안

● **개선방안**

허가신청서 최신화

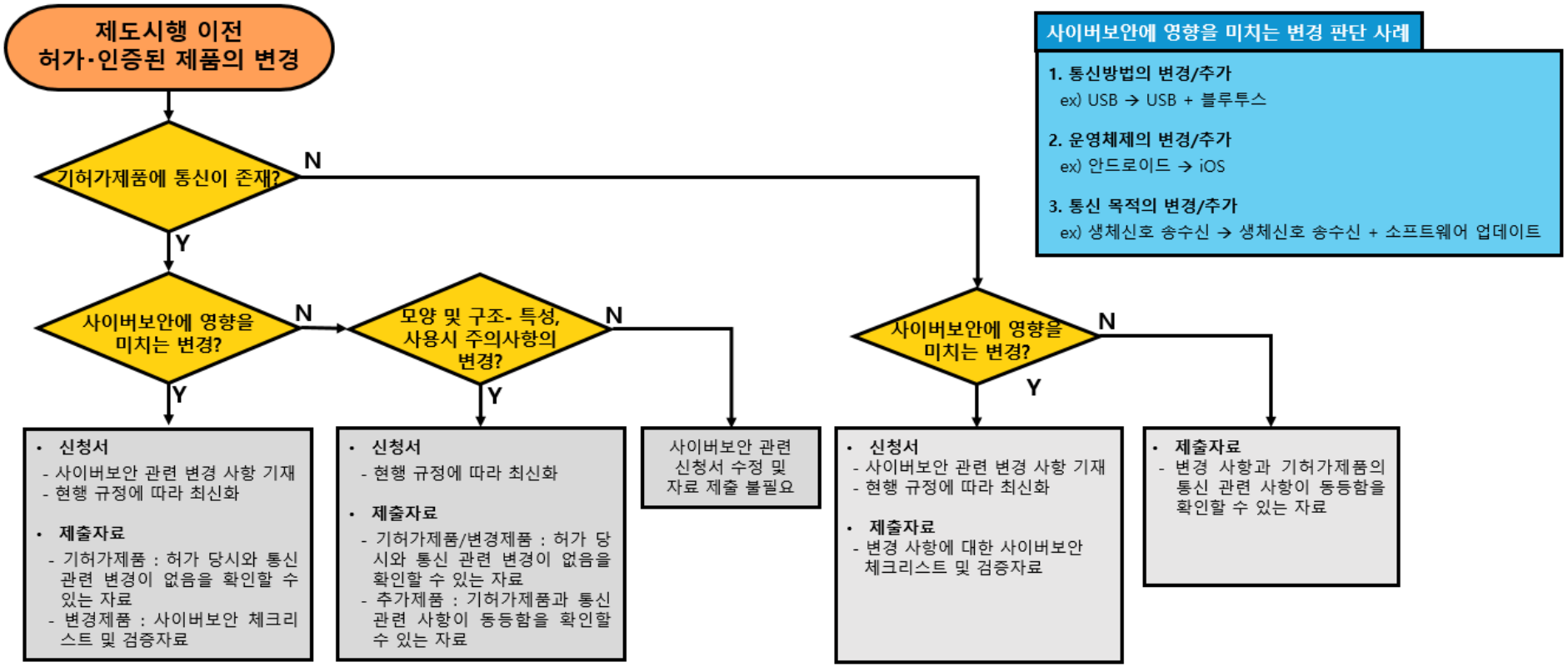
- **기허가 제품의 변경 신청일자 기준으로 최신 규정을 적용**
  - 통신 구성의 변경이 없더라도 현행 규정에 따라 통신구성도 및 사이버보안 사고 발생 시 대응 관련 문구 기재 요구

간소화된 사이버보안 자료 제출

- **기허가 제품과 통신 관련 사항이 동등함을 확인할 수 있으며, 제조원의 품질관리체계에서 관리되고 있는 자료 제출**
  - 제품 개발 및 설계문서 등

의료기기 변경 허가 시 제출자료 등 개선 방안

● 변경 흐름도



의료기기 변경 허가 시 제출자료 등 개선 방안

● 사례 1

- **허가 시점** : 제도 시행('19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : **소프트웨어 버전 변경(통신 관련 변경 X)**

의료기기 변경 허가 시 제출자료 등 개선 방안

사례1

- **허가 시점** : 제도 시행 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : 소프트웨어 버전 변경(통신 관련 변경 X)

제도시행 이전 허가·인증된 제품의 변경

기허가제품에 통신이 존재?

- N → **사이버보안에 영향을 미치는 변경?**
- Y → **사이버보안에 영향을 미치는 변경?**

사이버보안에 영향을 미치는 변경?

- N → **모양 및 구조- 특성, 사용시 주의사항의 변경?**
- Y

모양 및 구조- 특성, 사용시 주의사항의 변경?

- N → 사이버보안 관련 신청서 수정 및 자료 제출 불필요
- Y

사이버보안에 영향을 미치는 변경?

- N
- Y

사이버보안에 영향을 미치는 변경 판단 사례

1. **통신방법의 변경/추가**
   ex) USB → USB + 블루투스
2. **운영체제의 변경/추가**
   ex) 안드로이드 → iOS
3. **통신 목적의 변경/추가**
   ex) 생체신호 송수신 → 생체신호 송수신 + 소프트웨어 업데이트

- **신청서**
  - 사이버보안 관련 변경 사항 기재
  - 현행 규정에 따라 최신화
- **제출자료**
  - 기허가제품 : 허가 당시와 통신 관련 변경이 없음을 확인할 수 있는 자료
  - 변경제품 : 사이버보안 체크리스트 및 검증자료

- **신청서**
  - 현행 규정에 따라 최신화
- **제출자료**
  - 기허가제품/변경제품 : 허가 당시와 통신 관련 변경이 없음을 확인할 수 있는 자료
  - 추가제품 : 기허가제품과 통신 관련 사항이 동등함을 확인할 수 있는 자료

- **신청서**
  - 사이버보안 관련 변경 사항 기재
  - 현행 규정에 따라 최신화
- **제출자료**
  - 변경 사항에 대한 사이버보안 체크리스트 및 검증자료

- **제출자료**
  - 변경 사항과 기허가제품의 통신 관련 사항이 동등함을 확인할 수 있는 자료

의료기기 변경 허가 시 제출자료 등 개선 방안

● 사례 1

- **허가 시점** : 제도 시행 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : 소프트웨어 버전 변경(통신 관련 변경 X)

허가신청서 기재방법

- **현행 규정에 따라 최신화**
  - 통신구성도 및 사이버보안 사고 대응 관련 문구 기재

사이버보안 제출자료

- **사이버보안 동등성 입증 자료**
  - 허가 시점부터 USB포트가 존재하였으며, 통신 관련 변경 없음을 확인할 수 있는 자료 제출

의료기기 변경 허가 시 제출자료 등 개선 방안

● 사례 2

- **허가 시점** : 제도 시행('19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : **성능, 사용 방법 변경**

의료기기 변경 허가 시 제출자료 등 개선 방안

사례 2

- **허가 시점** : 제도 시행(19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : **성능, 사용 방법 변경**

제도시행 이전 허가·인증된 제품의 변경

기허가제품에 통신이 존재?
- N → **사이버보안에 영향을 미치는 변경?**
  - N → **모양 및 구조- 특성, 사용시 주의사항의 변경?**
    - N → 사이버보안 관련 신청서 수정 및 자료 제출 불필요
    - Y →
      - **신청서**
        - 현행 규정에 따라 최신화
      - **제출자료**
        - 기허가제품/변경제품 : 허가 당시와 통신 관련 변경이 없음을 확인할 수 있는 자료
        - 추가제품 : 기허가제품과 통신 관련 사항이 동등함을 확인할 수 있는 자료
  - Y →
    - **신청서**
      - 사이버보안 관련 변경 사항 기재
      - 현행 규정에 따라 최신화
    - **제출자료**
      - 기허가제품 : 허가 당시와 통신 관련 변경이 없음을 확인할 수 있는 자료
      - 변경제품 : 사이버보안 체크리스트 및 검증자료
- Y → **사이버보안에 영향을 미치는 변경?**
  - N →
    - **제출자료**
      - 변경 사항과 기허가제품의 통신 관련 사항이 동등함을 확인할 수 있는 자료
  - Y →
    - **신청서**
      - 사이버보안 관련 변경 사항 기재
      - 현행 규정에 따라 최신화
    - **제출자료**
      - 변경 사항에 대한 사이버보안 체크리스트 및 검증자료

사이버보안에 영향을 미치는 변경 판단 사례

1. **통신방법의 변경/추가**
   ex) USB → USB + 블루투스
2. **운영체제의 변경/추가**
   ex) 안드로이드 → iOS
3. **통신 목적의 변경/추가**
   ex) 생체신호 송수신 → 생체신호 송수신 + 소프트웨어 업데이트

의료기기 변경 허가 시 제출자료 등 개선 방안

● 사례 2

- **허가 시점** : 제도 시행('19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : **성능, 사용 방법 변경**

허가신청서 기재방법

- **현행 규정에 따른 최신화 불필요**

사이버보안 제출자료

- **사이버보안 동등성 입증 자료**
  - 허가 시점부터 USB포트가 존재하였으며, 통신 관련 변경 없음을 확인할 수 있는 자료 제출

의료기기 변경 허가 시 제출자료 등 개선 방안

● 사례 3

- **허가 시점** : 제도 시행('19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : **블루투스 통신 추가**

의료기기 변경 허가 시 제출자료 등 개선 방안

사례 3

- **허가 시점** : 제도 시행('19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : 블루투스 통신 추가

제도시행 이전 허가·인증된 제품의 변경

기허가제품에 통신이 존재?

- N → **사이버보안에 영향을 미치는 변경?**
  - N → **모양 및 구조- 특성, 사용시 주의사항의 변경?**
    - N → 사이버보안 관련 신청서 수정 및 자료 제출 불필요
    - Y →
      - **신청서**
        - 현행 규정에 따라 최신화
      - **제출자료**
        - 기허가제품/변경제품 : 허가 당시와 통신 관련 변경이 없음을 확인할 수 있는 자료
        - 추가제품 : 기허가제품과 통신 관련 사항이 동등함을 확인할 수 있는 자료
  - Y →
    - **신청서**
      - 사이버보안 관련 변경 사항 기재
      - 현행 규정에 따라 최신화
    - **제출자료**
      - 기허가제품 : 허가 당시와 통신 관련 변경이 없음을 확인할 수 있는 자료
      - 변경제품 : 사이버보안 체크리스트 및 검증자료
- Y → **사이버보안에 영향을 미치는 변경?**
  - N →
    - **제출자료**
      - 변경 사항과 기허가제품의 통신 관련 사항이 동등함을 확인할 수 있는 자료
  - Y →
    - **신청서**
      - 사이버보안 관련 변경 사항 기재
      - 현행 규정에 따라 최신화
    - **제출자료**
      - 변경 사항에 대한 사이버보안 체크리스트 및 검증자료

사이버보안에 영향을 미치는 변경 판단 사례

1. **통신방법의 변경/추가**
   ex) USB → USB + 블루투스
2. **운영체제의 변경/추가**
   ex) 안드로이드 → iOS
3. **통신 목적의 변경/추가**
   ex) 생체신호 송수신 → 생체신호 송수신 + 소프트웨어 업데이트

의료기기 변경 허가 시 제출자료 등 개선 방안

● 사례 3

- **허가 시점** : 제도 시행('19.11월) 이전 허가
- **기허가사항에 통신포트 존재 여부** : USB 통신 포트 존재
- **변경 사항** : 블루투스 통신 추가

허가신청서 기재방법

- **현행 규정에 따라 최신화**
  - 통신구성도 및 사이버보안 사고 대응 관련 문구 기재

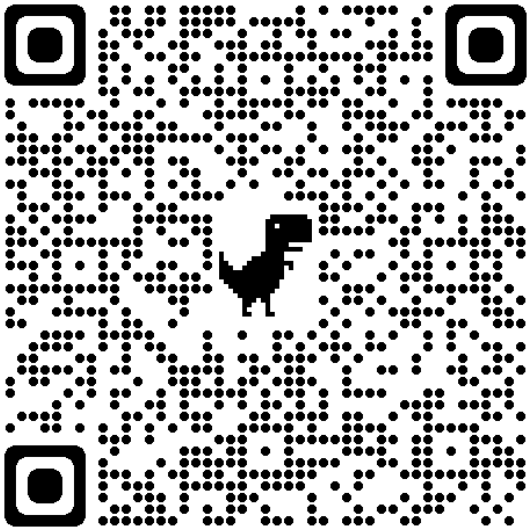
사이버보안 제출자료

- **USB 통신 기능**
  - 허가 시점부터 USB포트 존재하였으며, 통신 관련 변경 없음을 확인할 수 있는 자료 제출
- **블루투스 통신 기능**
  - 블루투스 통신 기능 관련 사이버보안 요구사항 체크리스트 및 검증자료 제출

식품의약품안전처

질의 응답

[참고] 설명회 평가



- **설명회 품질 향상을 위한 설명회 평가 및 의견 적극 협조 요청**