청렴韓세상

국민의 내일을 위한 정부혁신 보다 나은 정부

의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ)[민원인 안내서]

2021. 4. 22

식품의약품안전처
식품의약품안전평가원
의 료 기 기 심 사 부

지침서·안내서 제·개정 점검표

명칭	의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ)[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
	□ 일회성 지시·명령에 해당하는 내용입니까?	□ 예 ■ 아니오
	□ 외국 규정을 단순 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	□ 행정사무의 통일을 기하기 위하여 내부적으로 행정사무의 세부기준이나 절차를 제시하는 것입니까? (공무원용)	□ 예 ■ 아니오
	□ 민원인들의 이해를 돕기 위하여 법령 또는 행정규칙을 알기 쉽게 설명하거나 특정 민원업무에 대한 행정기관의 대외적인 입장을 기술하는 것입니까? (민원인용)	■ 예 □ 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.

2021 년 4 월 22 일

담당자 김 현 수

확 인(부서장) 강 영 규

제·개정 이력서

의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ) (민원인 안내서)

제・개정번호	승인일자	주요 내용
안내서-1114-01	2021.04.22	의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ)(민원인 안내서) 제정

이 안내서는 의료기기 사이버보안 관련 자주 묻는 질의사항 등에 대해 알기 쉽게 설명하거나 식품의약품안전처의 입장을 기술한 것입니다.

본 안내서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술 방식('~하여야 한다' 등)에도 불구하고 참고로만 활용하시기 바랍니다. 또한, 본 안내서는 '21년 4월 22일 현재의 과학적·기술적 사실 및 유효한 법규를 토대로 작성되었으므로 이후 최신 개정 법규 내용 및 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

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

※ 본 안내서에 대한 의견이나 문의사항이 있을 경우 의료기기심사부 첨단의료기기과 (디지털헬스기기팀)에 문의하시기 바랍니다.

전화번호 : 043-719-3942~3949

팩스번호 : 043-719-3940

목 차

Part 1 사이버보안 자료 제출 대상

가. 통신 목적에 따른 자료 제출 대상 여부

나. 통신 구성에 따른 자료 제출 대상 여부

다. 변경 시 자료 제출 대상 여부

Part 2 사이버보안 필수원칙 체크리스트

가. 통신 구성에 따른 적용 항목

나. 체크리스트 항목별 입증 방법

Part 3 사이버보안 안전성 입증 자료

가. 제출 자료의 요건 및 종류

나. 제출 자료에 포함되어야할 사항

Part. 01

사이버보안 자료 제출 대상

Q 1.1

제품에 LAN 포트가 장착되어 있지만, 외부 네트워크와의 통신 목적이 아니라 프린터만을 연결하기 위한 목적의 LAN 포트인 경우에도 사이버보안 자료 제출 대상인가요?

A. 신청제품과 프린터의 통신목적이 아래와 같은 사이버보안 적용 범위에 해당하면 사이버보안 자료 제출 대상입니다.

- 예1) 검사지 출력을 위한 치료 매개변수 송·수신(개인의료정보 송·수신)
- 예2) 기기 사용 기록 송·수신(소프트웨어 유지보수)

Q 1.2

전기수술기에서 제품의 품질개선을 위해 사용 후 제조원 서버로 데이터(환자 개인 정보를 포함하지 않는 제품 사용 시간 및 출력값 등의 통계 데이터)를 전송할 때에도 사이버보안 자료 제출 대상인가요?

A. 제품의 품질개선을 위한 통신은 소프트웨어 유지보수에 해당하므로 사이버보안 자료 제출 대상입니다.

Q 1.3

전기수술기의 유지보수(A/S)를 위한 소프트웨어 테스트 또는 디버깅을 위한 통신을 할 때에도 사이버보안 자료 제출 대상인가요?

A. 해당 통신은 소프트웨어 유지보수에 해당하므로 사이버보안 자료 제출 대상입니다.

Q 1.4

연성요관경 및 내시경용광원장치에서 HDMI 케이블과 같이 단순하게 영상을 컴퓨터 또는 영상장치로 전송해주는 유선 케이블 포트가 있는 경우에도 사이버보안 자료 제출 대상인가요?

A. 해당 제품은 유선 통신(HDMI)으로 개인의료정보(환자 의료 영상)를 송수신하므로 사이버보안 자료 제출이 필요합니다. 다만, 수술실과 같이 통제된 환경에서 제한된 시간에만 사용되는 의료기기는 위험분석을 통해 일부 항목의 안전성을 입증할 수 있습니다.

Q 1.5

1) 제조원의 담당 직원이 기기의 소프트웨어 업그레이드 또는 내부 스캔을 통해 오류를 확인하기 위해 사용되는 USB 포트가 있는 제품도 사이버보안 자료 제출 대상인가요?
2) 추가로, 이러한 USB 포트가 기기 내부에 있으며 외장 케이스를 제거하지 않으면 접근이 불가능한 경우에도 사이버보안 자료 제출 대상인가요?

A. 1) USB 포트의 통신목적이 소프트웨어 유지보수에 해당하므로 사이버보안 자료 제출 대상입니다.

2) USB, RS232, HDMI 등의 통신포트가 기기 내부에 있고 외장 케이스 등으로 덮여 있어 사용자의 접근이 불가능한 경우, 관련 자료(예. 기기 내부의 통신포트 사진 등)만으로 사이버보안 자료를 대체 할 수 있습니다. 다만, 무선 통신 및 LAN을 이용하는 경우 기기 내부에 위치하더라도 사이버보안 자료 제출 대상입니다.

Q 1.6

환자의 체온을 측정하는 체온계가 무선 통신을 이용해 환자 개인 정보(이름, 성별, 출생일 등)가 아닌 체온 데이터만을 다른 모니터링 장치에 전송하는 경우 이 체온계 제품도 사이버보안 자료 제출 대상인가요?

A. 개인의료정보는 당사자를 식별 가능한 그 개인에 대한 정보 뿐만 아니라 의료서비스를 위한 환자등록정보, 환자 의료에 대한 적격성이나 비용 지불에 대한 정보, 의료서비스 목적으로 환자를 식별할 수 있도록 지정된 숫자·심벌·기타 사항, 환자에게 의료서비스를 제공하기 위하여 수집된 그 개인의 정보, 신체부위나 신체적출물의 검사나 시험으로 얻어진 정보, 환자에게 의료 서비스를 제공하는 사람(의료인 등)에 대한 정보를 모두 포함합니다.

체온 데이터는 신체부위나 신체적출물의 검사나 시험으로 얻어진 정보에 해당하므로 해당 제품은 개인의료정보를 송수신하는 제품이며, 사이버보안 자료 제출 대상입니다.

Q 1.7

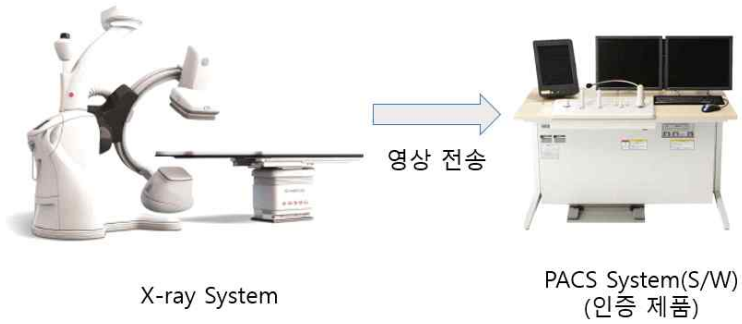
환자에게 공급되는 호흡가스의 온도와 습도를 조절하기 위한 의료용온습도조절기 제품 사용 중 발생하는 이벤트 기록을 저장하기 위해 SD 카드를 이용하는 경우에도 사이버보안 자료 제출 대상인가요?

A. 의료기기와 직접 통신할 수 없는 포트(SD 카드, CD, DVD 등)는 사이버보안 침해 가능성이 낮은 것으로 판단하여 사이버보안 자료를 제출을 요구하지 않습니다.

Q 1.8

엑스레이, CT 등 영상 획득 장치에서 획득한 영상을 별도의 PACS 시스템(별도 인증 제품)으로 보내는 제품의 경우 영상 획득 장치는 사이버보안 자료를 제출하지 않아도 되나요?

A.



영상 획득 장치에서 PACS로 데이터를 전송하기 위한 통신포트(LAN 포트 등)에 대해서는 사이버보안 자료 제출이 대상입니다. 다만, 특정 사용 환경(ex. 병원 폐쇄망 등)에서 통신하는 제품의 경우, 사이버보안 필수원칙 체크리스트 항목 중 일부 요구사항은 근거자료(위험관리 문서 등) 제출과 '사용 시 주의사항'의 특정 환경 및 특정목적 등을 함께 기재하는 것으로 대체 인정 가능합니다.

Q 1.9

사용자에게는 업그레이드 권한이 없고 제조자 시설에서만 펌웨어 또는 소프트웨어 업그레이드가 가능한 경우에도 사이버보안 자료 제출 대상인가요?

A. 소프트웨어 업그레이드 등 소프트웨어 유지보수를 위한 통신 기능이 있는 경우 사이버보안 자료 제출 대상입니다. 다만, 소프트웨어 유지보수를 위한 통신포트가 기기 내부에 위치하고 있고 외장 케이스 등으로 덮여 있어서 사용자의 접근이 불가능한 경우에는 관련 자료(예. 기기 내부의 통신포트 사진 등)만으로 사이버보안 자료를 제출할 수 있습니다.(단, 무선통신 및 LAN 통신 제외)

Q 1.10

의료영상저장전송장치(HW)에 공산품으로 인증받은 태블릿을 구성품으로 포함할 경우 사이버보안 자료 제출 대상인가요?

A. 상용 태블릿과 개인의료정보 송수신, 기기제어, 소프트웨어 유지보수를 위한 통신을 하는 경우 사이버보안 자료 제출 대상이며, 해당 제품의 통신목적에 해당하는 통신 방법에 대해서만 사이버보안 자료를 제출하면 됩니다.

- 예) 태블릿(LAN/USB 포트 등 포함)과 의료영상저장전송장치가 USB 포트만을 이용하여 개인의료정보를 송·수신하는 경우, USB 포트에 대한 사이버보안 자료만 제출

Q 1.11

에너지를 출력하는 장비(예:레이저수술기)에서 태블릿(옵션 구성품)을 통해 출력 직경이나 모양 및 출력값 등을 설정할 수 있으나 실제 출력(주성능)은 하드웨어 구성품을 통해서만 가능한 경우에도 사이버보안 자료 제출 대상인가요?

A. 제품에 개인의료정보 송수신, 기기제어, 소프트웨어 유지보수를 위한 유·무선 통신 기능이 있는 경우 사이버보안 자료 제출이 필요합니다. 다만, 전용 구성품(예 : 발판 스위치)을 이용하여야만 출력이 가능하도록 설계하여 사이버보안 위험을 경감시킨 경우 위험관리문서로 일부 항목에 대한 사이버보안 안전성 입증이 가능할 것으로 판단됩니다.

Q 1.12

홀뮴레이저가 RFID를 통하여 함께 사용되는 프로브를 인식하는 경우(어떤 모델이 사용되는지), 사이버보안 자료 제출 대상인가요?
또한, 바코드를 통해 환자정보(개인식별번호)를 획득하는 경우, 사이버보안 자료 제출 대상인가요?

A. RFID를 통하여 개인정보를 식별할 수 없는 경우에는(예. 제품의 추적 관리를 위한 RFID 태그 등) 사이버보안 자료 제출 대상이 아니며, 개인정보를 식별할 수 없더라도 개인의료정보 송수신(예. RFID를 통한 생체정보 송수신 등) 등의 기능을 하는 경우에는 사이버보안 자료 제출 대상입니다.

Q 1.13

공용 네트워크를 사용하지 않는 제품은 사이버보안 자료 제출 대상인가요?

A. 공용 네트워크(인터넷, wifi, 모바일 통신 등)를 사용하지 않더라도 개인의료정보 송수신, 기기제어, 소프트웨어 유지보수를 위한 유·무선 통신 기능(예. USB, 블루투스, RS232 통신 등)이 있는 경우에는 사이버보안 자료 제출대상입니다.

Q 1.14

유선통신 및 블루투스를 이용하여 기기(전기수술장치, 엑스레이 장비 등)의 동작을 제어하는 구성품(풋스위치 등)이 포함된 경우, 사이버보안 자료 제출 대상인가요?

A. 유·무선 통신을 이용하여 기기를 제어하는 경우에는 사이버보안 자료 제출 대상입니다. 다만 제품을 제어하기 위해 범용 통신 포트(LAN, USB, RS232 등)가 아닌 해당 제품에만 전용으로 사용되는 포트(예. 제조자 자체 제작 풋스위치, 핸드피스 케이블 등)일 경우에는 사이버보안 침해 가능성이 낮은 것으로 판단하여 사이버보안 자료 제출을 요구하지 않습니다.

Q 1.15

단독으로 사용되는 소프트웨어의 경우, PC에 설치되어 사용되고 있습니다. PC에는 네트워크에 직접 접속가능한 포트(LAN) 및 유지보수 등에 필요한 USB포트 등 입출력(SIP/SOP)포트가 있습니다. PC가 KS인증품인 경우, 사이버보안 자료 제출 대상인가요?

A. PC에 설치되어 단독으로 사용되는 소프트웨어가 개인의료정보 송수신, 기기 제어, 소프트웨어 유지보수를 위한 통신을 하는 경우 사이버보안 자료 제출 대상이며 해당 제품의 통신목적에 해당하는 통신 방법에 대해서만 사이버보안 자료를 제출하면 됩니다.

※ 예 : PC에는 LAN 포트, USB 포트, RS232 포트, HDMI 포트 등이 있으나, 해당 PC에 설치되는 독립형 소프트웨어는 LAN 포트만을 이용하여 개인의료정보를 송수신하고, 소프트웨어 업데이트를 수행하는 경우에는 LAN 포트에 대한 사이버보안 자료만 제출

Q 1.16

의료용진동기의 압력 및 온열 등을 조절하기 위해 적외선 통신을 사용하는 리모콘이 포함되는 경우, 사이버보안 자료 제출 대상인가요?

A. 적외선 통신은 리모컨과 기기 사이에 장애물 없이 근접하여 사용하여야만 통신이 가능하고, 사이버보안 침해로 발생할 수 있는 위험이 낮은 것으로 판단하여 사이버보안 자료 제출을 요구하지 않습니다. 다만, 제품의 위해도가 높아 사이버보안 안전성 등급 '상'에 해당되는 경우에는 사이버보안 필수원칙 체크리스트 항목 중 일부항목(접근통제 방식 등)에 대한 자료 제출이 필요합니다.

Q 1.17

의료기기와 별도의 PC용 소프트웨어가 USB 포트 등으로 연결되어 데이터를 송수신하는 제품에 대해 별도의 PC용 소프트웨어가 출시되지 않아 통신하는 소프트웨어가 없는 경우 사이버보안 자료 제출 대상인가요?

A. 의료기기에 통신 기능이 있는 경우에는 구성품 또는 별도의 PC용 소프트웨어 출시여부와 상관없이 사이버보안 자료 제출 대상입니다. 다만, 소프트웨어 출시 전까지 해당 통신 포트를 비활성화하는 경우 이를 검증한 자료(USB 통신핀이 연결되지 않은 회로도, 통신포트의 데이터 송수신 기능을 비활성화 시킨 소프트웨어 검증 및 유효성 확인자료 등)를 제출하면 통신기능이 없는 것으로 판단하여 사이버보안 자료 제출을 요구하지 않습니다.

Q 1.18

기허가 제품의 통신 포트가 변경 또는 추가되는 경우 사이버보안 자료 제출 대상인가요?

A. 제품의 통신방법 또는 통신목적이 변경/추가되면 사이버보안 자료 제출대상입니다.

- 통신방법 변경 예시)
  - USB → RS232, LAN 등
- 통신목적 변경 예시)
  - 소프트웨어 유지보수 → 소프트웨어 유지보수 및 기기제어
  - 비활성화 시킨 블루투스 모듈 → 기기제어를 위한 블루투스 통신 활성화

Q 1.19

통신 방법과 관련 없는 기능만 변경된 경우 사이버보안 자료 제출 대상인가요?

A. 통신 방법(예. USB → RS232, LAN 등) 및 통신목적(예. 소프트웨어 유지보수 → 소프트웨어 유지보수 및 기기제어)의 변경이 없는 경우에는, 사이버보안 자료 제출 대상이 아닙니다.

Part. 02

사이버보안 필수원칙 체크리스트

Q 2.1

제품이 병원 폐쇄망 내에서만 통신이 이루어지는 경우 사이버보안 필수원칙 체크리스트의 항목 중 제외되는 항목이 있나요?

A. 특정 사용 환경(ex. 병원 폐쇄망 등)에서 통신하는 제품의 경우, 사이버보안 필수원칙 체크리스트 항목 중 일부 요구사항은 근거자료(위험관리 문서 등) 제출과 '사용 시 주의사항'의 특정 환경 및 특정목적 등을 함께 기재하는 것으로 인정 가능합니다.(단, 웹 PACS*는 제외)

* 웹 PACS(Web Picture Archiving Communication System) : 각 의료 기관에 구축된 의료 영상 저장 통신 시스템(PACS)을 인터넷 기반의 웹 환경으로 연동한 것. 웹 팩스를 이용하면 언제, 어디서나 관련된 의료 영상을 판독, 조치할 수 있다.

※ '사용 시 주의사항' 예시 : 해당 소프트웨어는 데이터에 대한 암호화 통신을 하지 않는 제품으로 병원의 폐쇄망에서만 사용되어야 하며, 방화벽이나 백신 등 보안시스템이 갖춰진 PC를 사용할 것

Q 2.2

필수원칙 체크리스트 항목 '2.4 DDos 공격에 대한 방어' 는 공용 네트워크망을 사용하지 않는 경우 '해당없음' 으로 기재해도 되나요?

A. '2.4 DDos 공격에 대한 방어' 항목은 공용네트워크 망에 접속하여 의료기기를 실시간으로 제어하거나 환자 생명과 직접적으로 연관될 수 있는 정보를 실시간으로 송수신하는 제품의 경우에 적용되는 항목으로 이에 해당되지 않는 경우에는 '해당 없음'으로 기재 가능하며, 제품에 대한 관련 자료(위험관리 문서 등)를 통해 '해당없음'에 대한 사항을 입증하여야 합니다.

Q 2.3

진단폐활량계에 블루투스 통신모듈이 탑재되어 있고, 통신 목적은 '측정값 확인', '펌웨어 업데이트 또는 유지보수' 로 개인용으로만 사용을 하는데 "1.7 사용자(의료기기) 인증관리" 항목의 적용이 필요한가요?

A. 해당 제품은 사이버보안 자료 제출 대상이며 '1.7 사용자(의료기기) 인증관리' 항목 적용 대상입니다. 다만, 동 항목에 대한 위험이 허용 가능한 수준이라고 판단하는 경우에는 타당한 근거자료(위험관리문서 등)를 제출하여 해당 항목의 안전성을 입증할 수 있습니다.

Q 2.4

광섬유 등을 이용하여 환부에 빛을 비추는 내시경용 광원 장치의 경우, 의료기기 사이버보안 안전성 등급이 '하' 로 되어있습니다. 제품 외장에 네트워크에 직접 접속 가능한 LAN 포트가 있을 경우, 추가로 해당하는 사이버보안 요구사항을 강제로 적용시켜야 되나요?

A. 사이버보안 안전성 등급이 '하'라 하더라도 체크리스트 항목 중 해당되는 항목이 있을 경우에는 해당 항목에 대한 사이버보안 안전성을 입증하여야합니다.

Q 2.5

통신이 되는 USB, LAN 포트는 사이버보안 필수원칙 체크리스트 1.18 항목(물리적인 통신포트 침해의 최소화)에 따라 반드시 물리적으로 막아야 하나요?

A. 반드시 물리적인 방법으로 통신포트를 막아야하는 것은 아닙니다. 물리적인 잠금 장치가 아닌 다른 통제 조치(S/W에 대한 조치로 비밀번호 설정 등)를 이용하여 사이버보안 안전성을 입증할 경우 이에 대한 근거자료 제출로 동 항목의 안전성 입증을 대체할 수 있습니다.

Q 2.6

의료기기와 개인용 스마트기기가 블루투스 통신으로 기기 제어 및 개인 의료정보 송수신을 하는 경우, 사이버보안 필수원칙 체크리스트 “식별 및 보호” 항의 일부 항목(접근통제 및 인증, 비인가된 사용자 접속제한, 사용자 인증관리, 비밀번호 작성 규칙 강화, 비밀번호 하드코딩 금지, 비밀번호 노출 금지 등)에 대해 스마트기기 자체의 보안 프로그램과 개인 지문인식 등을 통한 접속 기능으로 대체하여 입증 가능한가요?

A. 상용 제품(PC, 태블릿, 모바일 등)의 사이버보안 대응 방안(보안 프로그램 및 보안 기능) 및 이를 검증한 자료(예. 지문 인식 기능으로 제품에 대한 접근이 통제됨을 실제 검증한 자료 등)로 제출 가능합니다.

Q 2.7

“1.15 네트워크상의 의료기기 제어정보 전송 기밀성 및 무결성 보장”, “1.16 네트워크상의 개인 의료정보 전송 기밀성 및 무결성 보장” 항목은 인터넷 웹사이트나 게이트웨이를 통한 연결에 대해서만 입증하면 되나요? 블루투스, USB 등 모든 연결에 대해 입증하여야하나요?

A. 1.15 및 1.16 항목의 ‘네트워크’는 인터넷, 모바일 통신 등 공용 네트워크망과 블루투스, wifi, USB 등 모든 통신 가능한 연결망을 의미합니다. 따라서 모든 통신 가능한 연결망에 대하여 동 항목의 안전성을 입증하여야합니다.

Part. 03

사이버보안 안전성 입증 자료

Q 3.1

유 · 무선 통신 기능이 없는 것이 명확한 경우, 사이버보안 필수원칙 체크리스트 작성 시 “해당사항 없음” 으로 기재한 항목에 대해 반드시 자료 제출로 입증해야 하나요?

A. 제품에 유·무선 통신기능이 없는 경우에는 사이버보안 자료를 제출하지 않아도 됩니다.

Q 3.2

기존 위험관리 보고서 내 사이버보안 항목이 포함되어 있는 경우, 해당 문서로 사이버보안 위험관리 보고서를 대체 가능한가요?

A. 사이버보안만을 위한 위험관리문서 등을 따로 작성하여 제출할 필요는 없으며, 위험관리문서, 성능시험자료, 소프트웨어 검증 및 유효성 확인자료에 사이버보안 안전성과 관련한 사항들이 포함된 자료를 제출 가능합니다.

Q 3.3

사이버보안이 적용되는 제품의 경우 사이버보안 필수원칙 체크리스트는 필수로 제출해야 하나요? 다른 대체할 자료가 있나요?

A. 사이버보안 필수원칙 체크리스트는 반드시 제출하여야하며 체크리스트에는 해당되는 사이버보안 요구사항, 적용여부, 적합성 입증방법, 해당 법규 및 규격, 첨부자료(문서번호)를 기재하여야합니다.

Q 3.4

미국 허가(510K) 시 제출하여 인정받은 사이버보안 관련 문서 및 사이버보안 위험관리문서를 국내 허가(인증) 시 사이버보안 자료로 제출 가능한가요?

A. 국내 허가·인증 시 사이버보안에 대한 안전성은 '사이버보안 허가심사 가이드라인'의 사이버보안 체크리스트 항목에 대해 반드시 입증해야하며, 미국 허가 시 제출한 사이버보안 관련 문서에서 사이버보안 필수원칙 체크리스트 항목에 대한 적합성 입증방법 등이 확인이 된다면 제출 가능합니다.

Q 3.5

제3자 전문기관의 사이버보안 인증을 받으면 해당 인증서 및 성적서로 사이버보안 자료를 제출할 수 있다고 들었습니다. 국내에 어떤 시험검사기관이 있으며, 신청방법을 알고 싶습니다.

A. 사이버보안 체크리스트 및 관련 자료(위험관리문서, 성능시험성적서, 소프트웨어 검증 및 유효성 확인 자료)로 사이버보안 전문기관에서 발급한 사이버보안 인증서 및 첨부자료(평가보고서 등)를 제출 가능합니다. 사이버보안 인증기관으로는 한국인터넷진흥원(KISA), 시험검사기관으로는 한국기계전기전자시험연구원(KTC)이 있으며 구체적인 신청절차는 해당 기관에 문의바랍니다.

Q 3.6

기술문서 작성 시 모양 및 구조-특성의 "통신 구성도"를 작동계통도에 포함하여 통신 흐름도 및 통신기능 등이 기재되어 있다면 별도로 구분하여 "통신 구성도"를 작성할 필요가 없나요?

A. '모양 및 구조 - 특성'의 작동계통도에서 제품의 통신기능 및 구조가 명확히 확인되는 경우에는 별도의 통신구성도를 작성하지 않아도 됩니다.

Q 3.7

사이버보안 안전성 등급은 제조자가 판단하나요?
제출 자료에 꼭 안전성 등급에 대한 내용이 있어야 하나요?

A. 제조자는 사이버보안 침해로 발생할 수 있는 잠재적 결함으로부터 사용자에게 영향을 끼칠 수 있는 위해를 식별하고 그 정도에 따라 사이버보안 안전성 등급을 결정해야 하며 이에 따라 안전성 등급을 체크리스트에 반드시 기재해야 합니다.

Q 3.8

상용화된 방화벽을 사용하는 경우 제조원에서 검증해야 하는 항목이 있는지, 심사 시에 상용제품 사용에 대한 자료를 제출해야 하나요?

A. 상용 제품은 사이버보안 자료 제출 대상이 아니지만, 상용 제품의 사이버보안 통제 조치(예. 상용 방화벽을 이용한 IP 차단 등)를 이용하여 해당 제품의 사이버보안 안전성을 입증하는 경우에는 상용 제품의 사이버보안 통제 방법에 대한 검증 자료(예. 상용 방화벽을 이용하여 실제 IP 차단을 검증한 자료 등)가 필요합니다.

Q 3.9

범용 PC, 태블릿의 운영체제(window, android. 등) 의 보안을 따르는 경우, 어떤 자료를 제출하여야 하나요?

A. 상용 제품의 사이버보안 통제 조치(예. PC의 비밀번호 설정 기능을 이용한 접근 통제 등)를 이용하여 의료기기의 사이버보안 안전성을 입증하는 경우에는 상용 제품의 사이버보안 통제 방법에 대한 검증 자료(예. PC의 비밀번호 설정 기능 없이는 제품에 접근이 불가함을 실제 검증한 자료 등)가 필요합니다.

의료기기 허가·심사 시 자주 묻는 사이버보안 질문집(FAQ) [민원인 안내서]

발 행 처	식품의약품안전평가원 의료기기심사부 첨단의료기기과 디지털헬스기기TF
발 행 일	2021년 4월 22일
발 행 인	서경원
편집위원장	이정림
편 집 위 원	강영규, 한영민, 손승호, 배영우, 김현수, 정병수, 김병남, 김정원
문 의 처	(28159) 충북 청주시 흥덕구 오송읍 오송생명2로 187 식품의약품안전평가원 의료기기심사부 첨단의료기기과(디지털헬스기기팀) 전화 : 043-719-3942~3949 팩스 : 043-719-3940