의료기기 사이버보안 허가심사 방안

2019. 11. 20. (수)

국민권익위원회가 함께하는 청렴韓세상

식품의약품안전처 식품의약품안전평가원

보다 나은 식약처

식품의약품안전처

목 차

식품의약품안전처

Ⅰ. 추진배경

통신 기반 의료기기 개발 동향

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

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

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

- 유무선 통신을 이용하여 수술용 기기를 제어

해외 규제 및 기술 동향

미국 FDA

- 사이버 보안 사전, 사후 등 가이던스 발간
- 디지털 헬스 이노베이션 액션 플랜(사이버 보안 포함)
- 사이버 보안 사고 관련 제품 리콜 발생

IEC/ISO

- 의료기기 및 의료분야 소프트웨어의 보안 관련 표준 제개정
- IEC 60601-1, IEC 62304 등

식품의약품안전처

Ⅱ. 허가심사 방안

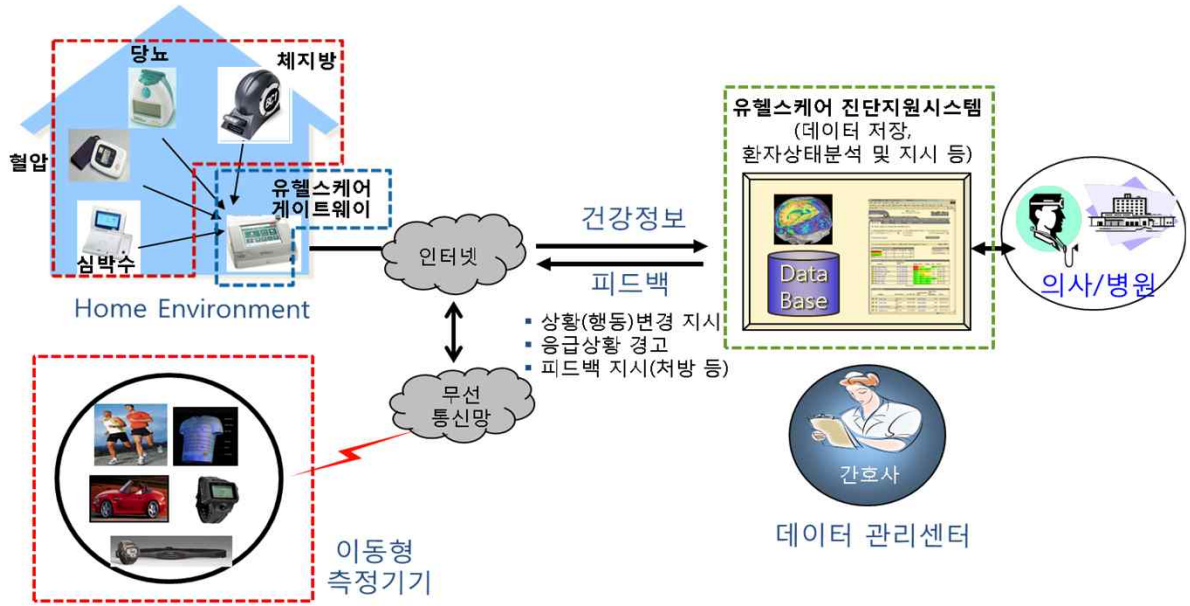
허가심사 방안 - 적용범위

유 · 무선 통신이 가능한 의료기기

1 유 · 무선 통신을 이용하여 환자의 생체정보 등 개인의료정보를 송수신 하는 의료기기

예시

유헬스케어 의료기기, 의료영상저장전송장치, 환자감시장치, 생체신호 측정용 의료기기 등



허가심사 방안 - 적용범위

유 · 무선 통신이 가능한 의료기기

2 **유 · 무선 통신을 이용하여 기기를 제어할 수 있는 의료기기**

예시

이식형심장박동기, 이식형인슐린주입기, 로봇수술기 등

허가심사 방안 - 적용범위

유 · 무선 통신이 가능한 의료기기

3 **유 · 무선 통신을 이용하여 펌웨어 또는 소프트웨어 업데이트 등 유지보수 하는 의료기기**

예시

레이저수술기, 초음파영상진단장치 등 유·무선 통신을 이용하는 대부분의 전자 의료기기

허가심사 방안 - 원칙

제조자는 의료기기의 사이버 보안을 보장하기 위하여

기밀성, 무결성, 가용성의 3대 원칙 준수 요구

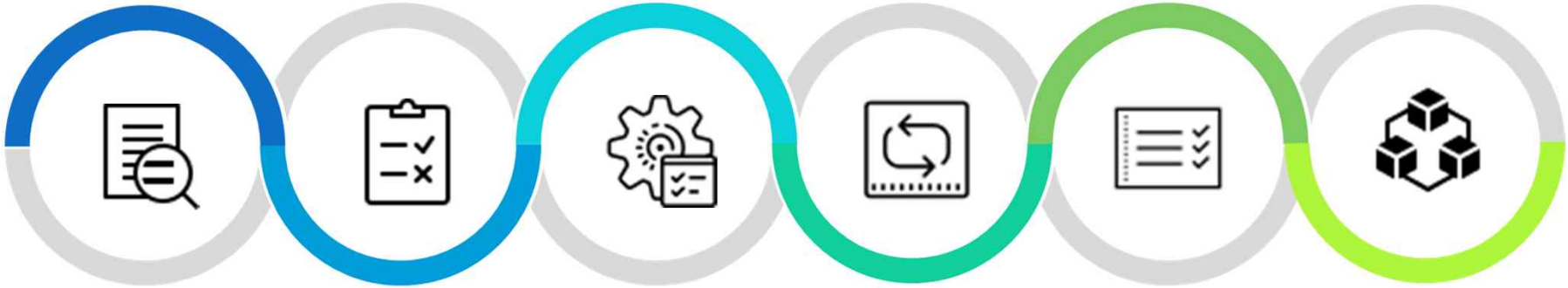
개인의료정보가 허가되지 않은 사람에게 공개되거나, 허가되지 않은 용도로 사용되지 않게 하는 기능

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 사이버 보안 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 – 차등 적용

의료기기 사이버 보안 안전성 등급

- 사이버 보안 침해로 인해 사용자에게 미치는 위해(harm)의 정도에 따라 사이버 보안 안전성 등급을 **3단계(상, 중, 하)로 구분**
- **등급별 요구사항**(상: 24개, 중: 23개, 하: 5개)을 **차등 적용**

허가심사 방안 - 요구사항

의료기기 사이버 보안 요구사항은 **식별, 보호, 탐지, 대응, 복구** 5단계로 분류하고,
각 분류별 세부 요구사항을 **총24개** 항목으로 제시

1. **식별**(Identify)
   제조자가 사이버 보안 위험을 확인하고 평가하는 과정
2. **보호**(Protect)
   사이버 보안을 보장하기 위해 필요한 보호 수단을 개발하는 과정
3. **탐지**(Detect)
   사이버 보안 사고 발생을 탐지할 수 있는 적절한 활동
4. **대응**(Respond)
   사이버 보안 사고에 대한 조치를 취하기 위해 필요한 활동
5. **복구**(Recover)
   의료기기 사이버 보안 사고로 손상된 의료기기의 기능을
   복구하기 위한 활동

허가심사 방안

사이버 보안 관련 시험에 대한 근거자료 활용

1. 의료기기 사이버 보안 필수 원칙 체크리스트	2. 사이버 보안 위험관리 문서	3. 소프트웨어 검증 및 유효성 확인 자료
• 의료기기 **사이버 보안 요구사항에 대한 적합성 여부**를 확인할 수 있는 자료 • 의료기기 사이버 보안 **필수원칙 체크리스트 양식을 활용하여 제품의 특성에 맞게 작성**하여 제출	• 의료기기 전체 생명주기에서의 사이버 보안과 관련된 위해요인을 파악하여 **발생 가능한 위해를 최소화 및 차단하기 위한 위험관리 활동**을 기록한 보고서 • 사이버 보안과 관련된 위해요인 식별과 각 위해요인에 대한 위험분석, 위험 경감 조치 결과 기재	• 의료기기 위험관리 과정에서 식별된 위해요인에 대한 **위험통제 조치의 결과를 검증할 수 있는 객관적인 자료** • 사이버 보안 요구사항에 대한 시험, 검증절차, 시험결과 등 포함

허가심사 방안 - 요구사항

1. 의료기기 사이버 보안 필수원칙 체크리스트

< 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 :

제품의 기술적 특성 상 요구사항이 제외 또는 추가 가능

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.				

요구사항이 제외 또는 추가되는 경우 적절한 사유를 '적합성 입증 방법'란에 기재

감사합니다.

[부패·공익신고 안내] ※ 신고자 및 신고내용은 보호됩니다.

‣ 식약처 홈페이지 “국민소통 > 신고센터 > 부패·공익신고 상담”코너

국민권익위원회가 함께하는 청렴韓세상

식품의약품안전처 식품의약품안전평가원

보다 나은 식약처