의료기기 허가심사과정 상 사이버보안 적용

- 사이버보안 요구사항 증대 및 위험관리 대응 필요 -

IT 기술이 접목된 의료기기에 대해 사이버보안 이슈가 발생한 경우 환자 개인정보의 유출 등 개인정보가 침해되는 것을 넘어서 기기의 오작동 등으로 환자 건강에 직접적인 위해가 있을 수도 있습니다. 이에 의료기기의 사이버 보안은 날로 그 중요성이 증가하고 있으며, 악의적 공격으로부터 환자 정보와 안전을 보호하기 위한 규제와 적용이 강화되고 있습니다. 의료기기의 허가 심사 과정에서 사이버보안 안전성 검토가 중요시되며, 변경 시에도 사이버 보안 측면에서 검토 절차가 엄격히 진행될 것으로 예상됩니다. 기업으로서는 최근 개정된 의료기기의 사이버 보안 허가/심사 가이드라인을 활용하여 사이버 보안이 요구되는 의료기기의 적용 대상을 명확히 파악하고 제품에 따라 적용가능한 보안 요구사항을 면밀히 검토해야 합니다.

1. **의료기기 사이버보안 개요**
   가. 배경
   나. 의료기기 사이버보안 규제 현황
2. **의료기기 허가심사 적용 방법 및 사례**
   가. 사이버보안 안전성 확인을 통한 의료기기 허가심사 강화
   나. 심사 및 변경허가 사례
3. **시사점**

1. 의료기기 사이버보안 개요

가. 배경

ICT 기술의 발달과 더불어 의료분야도 눈부신 발전을 거듭하고 있습니다. 의료기술과 IT의 융합으로 모바일 의료용 앱, 이식형 의료기기, U헬스케어 의료기기, 수술용 기기 등을 통해 개인 의료정보나 생체신호를 외부로 전달하고 유무선 통신을 이용하여 기기를 원격으로 제어할 수 있습니다.

의료기기가 악용될 경우 환자 또는 개인의 정보를 수집하는 것을 넘어서 기기를 조작하여 환자 건강에 직접적인 위해를 가할 수도 있는 것이 의료분야의 사이버 위협이며, 이러한 악의적 행위에 대해 환자의 생명을 보호하는 것이 의료분야 사이버 보안입니다. 대표적인 의료분야의 사이버 위협은 환자 몸에 이식하는 의료기기를 조작(2019년 인슐린 펌프 설정 변경, 2017 이식형 심장 박동기 조작 사례 등) 하거나, 의료기관의 전산망을 공격하여 정보 유출 또는 랜섬웨어 공격이 주를 이루었습니다.

본 내용은 일반적인 정보의 제공만을 목적으로 발행되므로 이에 수록된 내용은 저희 법인의 공식적인 견해나 구체적 사안에 관한 법률의견이 아님을 밝혀드립니다.

나. 의료기기 사이버보안 규제 현황

의료기기의 사이버 보안 적용을 위하여 국내/외에서도 의료분야 서비스의 효과성과 안전성을 검증함과 동시에 안전한 서비스에 대한 기획, 설계가 진행되고 있고, 그에 대한 기준 및 가이드가 발간되고 있습니다.

주요국들은 정부내 별도 조직을 구성하여 안전한 의료 데이터 수집 및 활용을 위한 기반마련을 중점으로 정책을 추진 중입니다. 디지털 헬스케어 산업내 사이버 보안은 대표적으로 IMDRF의 '의료기기 사이버보안 원칙 및 지침'이 있으며 의료기기 사이버보안의 일반 원칙을 제공하고 개발과 판매 후 관리에 대한 모범 사례에 관한 이해관계자를 위한 권고안을 제시하였습니다.

국내에서는 `18.05에 한국인터넷진흥원에서 '스마트의료 사이버보안 가이드'를 시작으로 `19.11월 의료기기허가 고시'가 개정되어 허가 시 사이버보안 자료 제출이 의무화되었습니다. 최근에는 `23년 식품의약품 안전처에서 '의료기기 사이버보안 허가심사 가이드라인'이 개정되어 의료기기 사이버보안을 위해 규제, 가이드 및 사례집을 공개하여 의료기기 사이버보안 적용에 노력하고 있습니다.

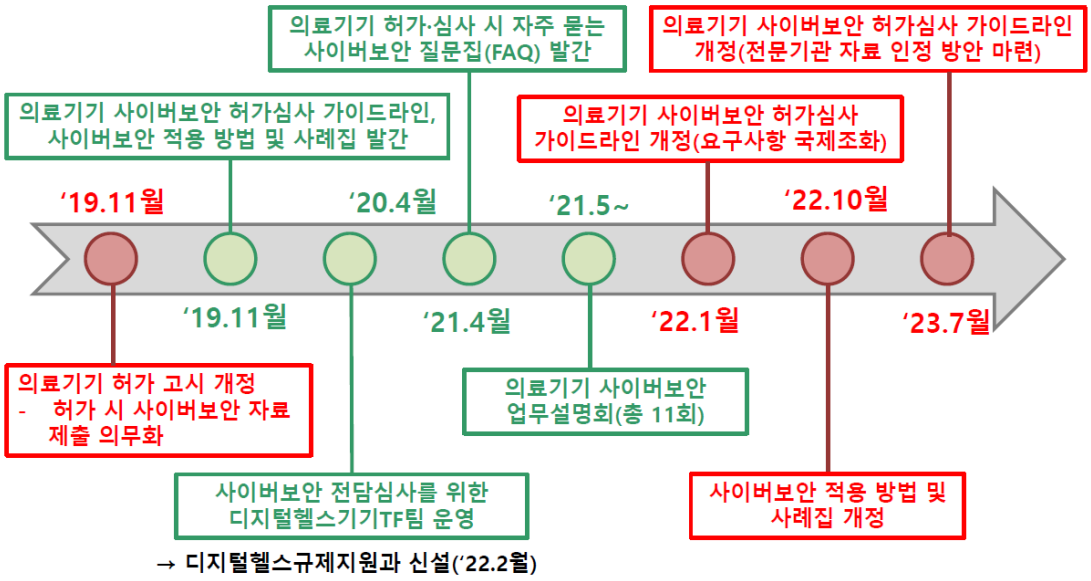

Figure 1. 의료기기 사이버보안 정책 추진 현황 (출처:식품의약품안전처 의료기기 사이버보안 업무 설명회)

2. 의료기기 허가심사 적용 방법 및 사례

가. 사이버보안 안전성 확인을 통한 의료기기 허가심사 강화

소프트웨어를 포함하는 통신 가능한 의료기기에 사이버 보안 적용하기 위하여 프로그램 가능 논리 제어기(PLC: Program Language Control)를 포함하는 의료기기, 소프트웨어(펌웨어)를 포함하는 의료기기, 스마트워치에서 측정된 혈압을 표시하는 소프트웨어 의료기기 등이 적용 대상입니다.

의료기기의 사이버보안 보장을 위하여 '기밀성', '무결성', '가용성'의 3대 원칙 준수를 위하여 의료기기 제조품질 관리체계의 위험관리 프로세스를 통해 사이버보안을 적용하게 됩니다.

본 내용은 일반적인 정보의 제공만을 목적으로 발행되므로 이에 수록된 내용은 저희 법인의 공식적인 견해나 구체적 사안에 관한 법률의견이 아님을 밝혀드립니다.

Figure 2. 의료기기 사이버보안 적용 절차 (출처: 식품의약품안전처 의료기기 사이버보안 업무 설명회)

제품 허가심사시 사이버보안 안전성을 확인하기 위하여 ① 의료기기 사이버보안 요구사항 체크리스트, ② 사이버보안 요구사항을 검증한 자료(소프트웨어 검증 및 유효성 확인 자료, 사이버보안 위험관리 문서, 성능시험성적서 등), ③ 사이버보안 요구사항 미적용 근거를 확인할 수 있는 자료(사이버보안 위험관리 문서 등)가 제출되어야 하며 세부 내용은 아래 심사 및 변경허가 적용 사례에서 예시를 통해 설명드리겠습니다.

나. 심사 및 변경허가 적용 사례

① 의료기기 사이버보안 요구사항 체크리스트는 `23.07 식품의약품안전처에서 발간한 '의료기기의 사이버보안 허가/심사 가이드라인'내에서 확인할 수 있으며 '보안통신' 부터 '신뢰성 및 가용성'까지 7개의 구분으로 세부 체크리스트는 15개로 의료기기 제조사입장에서의 기기의 안전성을 담보할 수 있도록 설계되었는지를 입증하게 됩니다.

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

Figure 3. 사이버보안 요구사항 체크리스트 작성 사례(출처: 식품의약품안전처 의료기기 사이버보안 업무 설명회)

② 사이버보안 요구사항을 검증한 자료'는, 소프트웨어 적합성 확인 보고서에 통신기능에 대한 목적을 작성하고 사이버보안 기술적 특성을 기재합니다. 그리고 의료기기의 위험관리 프로세스에 따라 '위험분석', '위험평가', '위험통제', '잔여위험 허용평가', '생산 및 생산 후 정보'의 단계로 진행됩니다. 산출물은 위험관리 절차의 최종 검토결과를 요약한 '**위험관리 보고서**'와 제품 설계 및 공정에서 발생할 수 있는 잠재적인 고장모드와 영향을 확인할 수 있는 **FMEA(Failure Mode and Effects Analysis)** 보고서를 작성합니다.

본 내용은 일반적인 정보의 제공만을 목적으로 발행되므로 이에 수록된 내용은 저희 법인의 공식적인 견해나 구체적 사안에 관한 법률의견이 아님을 밝혀드립니다.

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

Figure 4. 의료기기 위험평가 보고서 예시(출처:식품의약품안전처_의료기기의 사이버보안 적용방법 및 사례집)

③ 마지막으로, 의료기기 변경 허가시에는 통신기능 여부, 운영체제, 통신목적과 기타 모양 및 구조의 변경이 있는 경우 아래와 같은 절차도에 따라 신청서와 제출자료를 추가 제출합니다.

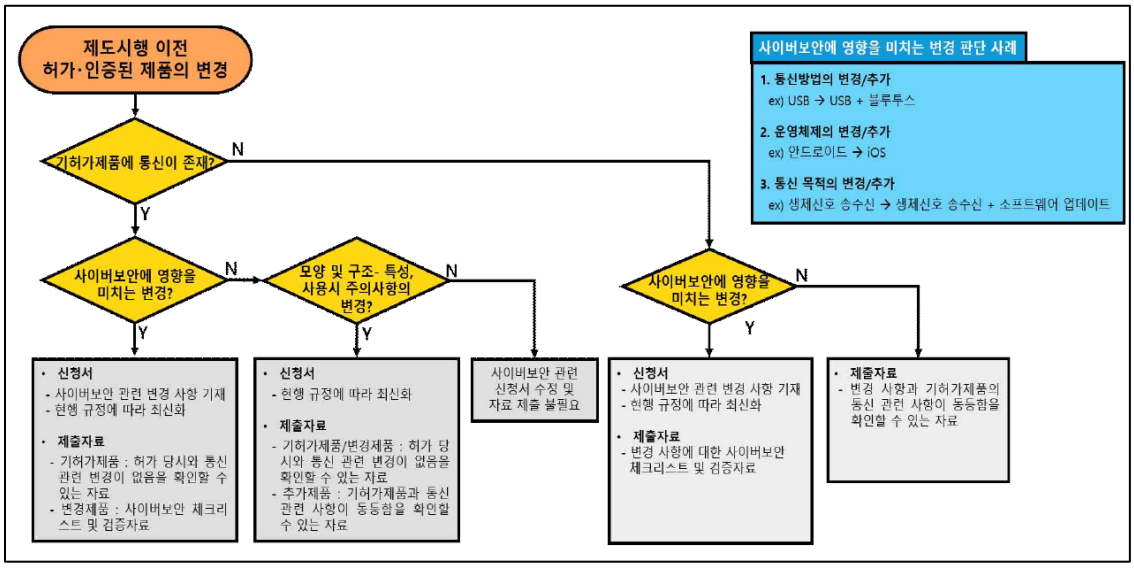

Figure 5. 의료기기 변경 허가 시 변경 흐름도(출처:식품의약품안전처_의료기기의 사이버보안 허가 · 심사 가이드라인)

3. 시사점

의료기기와 IT기술의 접목으로 의료기기의 통신의 취약점이나 소프트웨어의 취약점을 악용한 공격 사례들이 다수 발견되고 있습니다. 의료기기에 대한 사이버보안 안전성확보는 우리의 생명과도 직결될 수 있음으로 사용자를 위한 안전성 확보가 매우 중요하고 필수적입니다.

개정된 의료기기의 사이버 보안 허가/심사 가이드라인을 활용하여 사이버 보안이 요구되는 의료기기의 적용 대상을 명확히 파악하고 제품에 따라 적용가능한 보안 요구사항을 검토하여 의료기기의 해킹 · 정보유출· 오작동 유발 등의 정보보호 위협으로부터 안전하게 사용하는 될 수 있기를 기대하며, 앞으로도 기술발전과 규제 정책 동향 모니터링을 통해 의료분야의 사이버 보안 위협 요소를 파악하고 안전한 의료서비스 제공할 수 있도록 정보를 공유해 드리도록 하겠습니다.

본 내용은 일반적인 정보의 제공만을 목적으로 발행되므로 이에 수록된 내용은 저희 법인의 공식적인 견해나 구체적 사안에 관한 법률의견이 아님을 밝혀드립니다.

화우 정보보호센터는 오랜 경험과 축적된 노하우를 기반으로 기업 고객을 위한 최적의 솔루션을 안내해 드리고 있습니다. 정보보호 관련 법령의 해석 및 그 대응과 정보보호 기술적 자문(해킹 진단, 보안취약점) 등 포괄적인 올인원(All-in-One) 서비스를 제공하고 있습니다. 관련하여 문의사항이 있으신 경우 언제든지 화우에 연락하여 주시기 바랍니다.

Contacts

이근우
센터장/파트너변호사
T. (+82) 2 6003 7558
E. klee@yoonyang.com

이광욱
파트너변호사
T. (+82) 2 6003 7535
E. kwlee@yoonyang.com

이수경
파트너변호사
T. (+82) 2 6182 8132
E. sgyi@yoonyang.com

정호선
변호사
T. (+82) 2 6182 8548
E. junghs@yoonyang.com

백재환
전문위원
T. (+82) 2 6182 8366
E. jhb@yoonyang.com

지재원
연구위원
T. (+82) 2 6003 7568
E. jwji@yoonyang.com