

디지털 의료기기 전자적 침해 행위
보안 지침

1. 제정이유

「디지털의료제품법」 제정(법률 제20139호, 2024. 1. 23. 공포, 2025. 1. 24. 시행) 및 「디지털의료제품법 시행규칙」에 따라 디지털의료기기 전자적 침해행위 보안지침에 관하여 필요한 사항을 규정하려는 것임

2. 주요내용

가. 보안활동 및 문서화(안 제2조)

디지털의료기기의 취약점을 지속적으로 감시하고 전자적 침해행위에 대응하기 위한 보안활동 및 문서화에 대한 세부 내용을 마련함

나. 물리적 보안체계(안 제3조~제5조)

보안 통신, 권한 및 인증 등 물리적 보안체계에 관한 규정을 마련함

다. 기술적 보안체계(안 제6조~제12조)

파일 및 입력 유효성, 데이터 보안, 암호화 키 관리 등 기술적 보안체계에 관한 규정을 마련함

라. 위험 관리(안 제13조~제16조)

제품 개발 전주기에 걸쳐 위험 관리 활동에 대한 세부 내용을 마련함

마. 전자적 침해행위의 대응(안 제17조~제19조)

전자적 침해행위에 대응하기 위한 계획 수립과 방안에 대하여 세부 내용을 마련함

바. 취약점 감시 및 대응(안 제20조~제22조)

디지털의료기기의 취약점을 감시하고 대응하기 위한 세부 내용을 마련함

사. 재검토 기한(안 제23조)

디지털의료기기 전자적 침해행위 보안지침에 대한 타당성 검토를 위하여 규정을 마련함

3. 의견 제출

이 제정규칙안에 대하여 의견이 있는 단체 또는 개인은 다음 사항을 기재한 의견서를 2025년 1월 6일까지 식품의약품안전처장(참조 : 디지털의료제품TF)에게 제출하여 주시기 바랍니다.

가. 입법예고 사항에 대한 항목별 의견(찬·반 의견과 그 이유)

나. 성명(단체인 경우에는 단체명과 대표자 성명), 주소 및 전화번호

다. 의견제출 방법 : 전자우편, 우편 또는 팩스, 전자공청회

1) 전자우편(이메일) : shhyun0606@korea.kr

2) 주소 : (28159) 충청북도 청주시 흥덕구 오송읍 오송생명2로 187 식품의약품안전처 디지털의료제품TF

3) 팩스 : 043-719-3780

라. 동 고시는 「디지털의료제품법 시행령」의 재입법예고(2024. 11. 20. ~ 2024. 12. 5.) 및 「디지털의료제품법 시행규칙」 재입법예고(2024. 11. 20. ~ 2024. 12. 10.)의 내용을 반영한 것으로 향후 상기 법령안이 변경될 경우에는 동 제정 고시안도 변경될 수 있습니다.

마. 규제영향분석서는 행정예고 기간 동안 의견 수렴, 규제연구센터의 비용분석 검증, 영향평가 등을 거쳐 보완될 예정으로 최종분석자료가 아님을 알려드립니다.

※ 제정령안에 대한 자세한 내용을 참고하고자 할 경우 식품의약품안전처 홈페이지(<http://www.mfds.go.kr>) 『법령·자료 - 입법/행정예고』란을 참고하여 주시기 바랍니다.

디지털의료기기 전자적 침해행위 보안 지침안

제1장 총 칙

제1조(목적) 이 지침은 「디지털의료제품법」 제14조 및 제32조에 따라 디지털의료기기를 전자적 침해행위로부터 안전하게 보호하기 위하여 디지털의료기기의 취약점을 지속적으로 감시하고 전자적 침해행위에 대응하는 물리적·기술적 관리체계 구축에 필요한 사항을 규정함을 목적으로 한다.

제2장 보안활동 및 문서화

제2조(보안 활동의 문서화) 「디지털의료제품법」 제14조제2항에 따른 디지털의료기기제조업자등(이하 “디지털의료기기제조업자등”이라 한다)은 디지털의료기기(디지털의료기기를 구성하는 액세서리, 전자 인터페이스 및 구성품을 포함한다. 이하 같다)를 전자적 침해행위로부터 안전하게 보호하기 위하여 동 지침을 고려하여 다음 각 호의 보안 업무를 수행하고, 이를 문서화하여야 한다.

1. 물리적·기술적 보안 체계 수립
2. 전자적 침해행위 대응
3. 위험 관리, 개발 및 검증, 레거시 관리 등 보안 활동
4. 침해사고 대응 및 취약점 감시

제3장 물리적 보안체계

제3조(물리적 보안) ① 디지털의료기기제조업자등은 디지털의료기기와의 운영 환경에서의 설치, 작동, 네트워크, 제품 관련 장비 및 자료 보호 등을 위한 물리적 보안 구성을 고려하여야 한다.

② 디지털의료기기제조업자등은 디지털의료기기를 운영하는 물리적 보안 환경을 분석하고 각종 물리적 위협으로부터 보호할 수 있도록 대책을 마련하여야 한다.

③ 디지털의료기기를 운영하는 환경이 비인가자 접근 통제, 출입 기록 관리 등의 접근 통제가 정의된 인가 절차 등에 따라 이루어지는지 확인해야 하며, 주요 시설(전산실 등)에 위치할 경우 이에 대한 물리적 보안 조치를 하여야 한다.

제4조(보안 통신) 디지털의료기기제조업자등은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 운영 환경의 보안 통신 방안을 마련하여야 한다.

1. 유·무선 네트워크 사용 시, 디지털의료기기 및 그 운영 환경의 네

트위크 보안 설정

2. 이동식 저장매체(USB 등)에 대한 물리적 제한
3. 보안을 고려한 내·외부 통신망(통신 구간 암호화, 암호화 프로토콜 사용 등) 구성 방안

제5조(권한 및 인증) 디지털의료기기제조업자들은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 운영 환경의 권한 및 인증 방안을 마련하여야 한다.

1. 사용자 접근 통제 강화 및 계정별 권한 설정
2. 세션 종료, 중복 로그인 방지 등 로그인 세션 및 쿠키 설정
3. 미승인 기기 접근 제한 등 신원 확인을 위한 인증 사용
4. 원격 접속 차단 또는 제한된 원격 접속 조치(사용자 인증, 보안 통신 사용 등)

제4장 기술적 보안체계

제6조(기술적 보안) ① 디지털의료기기제조업자들은 디지털의료기기 및 그 운영 환경, 네트워크, 제품 관련 장비 및 자료보호 등을 위한 기술적 보안 사항을 고려하여야 한다.

② 디지털의료기기제조업자들은 디지털의료기기가 운영되는 기술적 보안 환경을 분석하고 각종 기술적 위협으로부터 보호할 수 있도록 대책을 마련하여야 한다.

③ 디지털의료기기제조업자들은 개인정보 또는 개인정보가 포함된 데

이터 취득 또는 보관 시, 개인정보 보호를 위한 조치를 하여야 한다.

제7조(파일 및 입력 유효성) 디지털의료기기제조업자등은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 운영 환경의 중요 파일 및 입력 유효성 확보 방안을 마련하여야 한다.

1. 파일을 업로드하는 경우 파일 확장자, 형식 등 유효성 및 무결성 검증
2. 파일을 다운로드하는 경우 해시값 비교 등 원본 파일과의 동일 여부
 부에 대한 유효성 및 무결성 검증
3. 디지털의료기기에서 작동 가능한 실행 파일 업로드 방지
4. 입력 데이터 검증, 버퍼 초과 오류 검증 등 입력 정보의 유효성 검증

제8조(데이터 보안) 디지털의료기기제조업자등은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 디지털의료기기가 작동하는 운영 환경의 중요 데이터 보안 방안을 마련하여야 한다.

1. 안전한 데이터베이스 패스워드 설정, 패스워드의 주기적 변경, 미사용 중인 관리자 계정 삭제 등 데이터베이스 보안 관리
2. 개인정보에 대한 암호화 등 데이터 비식별화 조치
3. 시스템 간 데이터 송수신 시, 데이터 암호화 또는 보안 통신 적용
 등 암호화 조치
4. 국내·외 암호화 알고리즘 사용 시, 널리 권고되는 암호화 및 해시
 알고리즘 사용

제9조(암호화 키 관리) 디지털의료기기제조업자등은 다음 각 호의 사항

을 고려하여 디지털의료기기 및 그 운영 환경의 암호화 키 관리 방안을 마련하여야 한다.

1. 암호화 키와 암호화된 데이터와의 분리 조치 방안, 암호화 키 유효기간 설정 등 암호화 키 보안 조치
2. 암호화 키 보호용 제어 장치 또는 시스템(하드웨어 등) 적용

제10조(유지 관리) 디지털의료기기제조업자등은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 운영 환경의 유지 관리 방안을 마련하여야 한다.

1. 디지털의료기기 자체 또는 연관 소프트웨어(운영체제, 제3자 소프트웨어, 오픈소스 등) 업데이트 파일에 대한 안전성 및 무결성 검증
2. 디지털의료기기 업데이트 실패에 대한 대응(복구 기능 제공 등) 방안
3. 디지털의료기기 자체 또는 연관 소프트웨어의 비 인가된 변경에 대한 무결성 검증 방안

제11조(보안 모니터링 및 대응) ① 디지털의료기기제조업자등은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 운영 환경의 보안 모니터링 및 대응 방안을 마련하여야 한다.

1. 불필요한 서비스(인터페이스) 등 비활성화, 보안 모니터링 기능 구현 등 대응 방안
2. 소스코드 및 주요 운영 데이터 백업 및 복구 방안
3. 컴퓨터 등 최신 버전의 안티 바이러스 소프트웨어 설치 여부
4. 로그 및 백업/복구 등 관리 방안

② 의료서비스제공자는 디지털의료기기 및 그 운영 환경에 대한 보안 모니터링을 수행하고 보안 문제 발생 시 제20조제2항에 따라 디지털의료기기제조업자등에게 알릴 수 있다.

제12조(인공지능 보안) 디지털의료기기제조업자등은 다음 각 호의 사항을 고려하여 디지털의료기기 및 그 운영 환경의 인공지능 보안 방안을 마련(인공지능기술이 적용된 디지털의료기기에 한한다)하여야 한다.

1. 데이터 중독 공격, 회피 공격 등과 같은 데이터 공격에 대한 방어 수단
2. 학습 데이터 수집, 구축 및 보관 과정에서의 데이터 변형, 데이터 조작 등의 위변조 행위에 대한 방어 수단
3. 반복된 질의 조회 차단, 적대적 공격 판단 모델 구현 등 인공지능 모델 추출/회피 공격 대응 방안
4. 인공지능 시스템 운영 중 문제 발생 시 피드백 제공 화면 전환, 이용자 안내 메시지 제공, 인공지능 기술이 적용된 주요 기능의 중단 등 운영 대응 방안

제5장 위험 관리

제13조(위험 관리 활동) ① 디지털의료기기제조업자등은 다음 각 호의 사항을 포함하여 제품 개발 전주기에 걸쳐 위험 관리 활동을 수행하여야 한다.

1. 제품 수명 주기 전반적인 위험 모델링

2. 위협 및 취약점에 대한 식별 및 위협 평가
3. 보안 위협 완화를 위한 위협 통제 조치 설계, 구현 및 검증
4. 잔여 위협 평가 및 평가 보고서 작성
5. 시판 후 위협 및 취약점 모니터링

② 의료서비스제공자는 제품 사용 도중 확인된 위협 및 취약점에 대해 디지털의료기기제조업자등과 협력하여 위협 관리 활동을 지원할 수 있다,

제14조(개발 및 검증 활동) ① 디지털의료기기제조업자등은 보안 코딩 표준, 보안 설계, 보안 테스트, 취약점 테스트 등 보안 요구사항을 고려하여 제품을 개발 및 검증하여야 한다.

② 디지털의료기기제조업자등은 검증 활동에 사용하는 테스트 도구에 대한 유효성을 확인하여야 한다.

③ 디지털의료기기제조업자등은 필요한 경우 제1항 내지 제2항의 개발 및 검증 활동에 대한 문서를 의료서비스제공자에게 제공할 수 있다.

제15조(레거시 디지털의료기기 관리 활동) ① 디지털의료기기제조업자등은 전자적 침해행위에 대비하여 디지털의료기기를 개발하는 경우 지원 종료 이후 보안 위험을 최소화하도록 디지털의료기기를 설계 및 구현하여야 한다.

② 디지털의료기기제조업자등은 제품 출시 이후 예상 지원 종료 일정과 수명 종료 이후 예상 지원 계획 등에 대해 의료서비스제공자에게 제공하여야 한다.

③ 디지털의료기기제조업자들은 의료서비스제공자에게 제품 수명 종료 단계 내에서 위험 및 취약점이 발견되는 경우 의료서비스제공자와 협력하여 이를 해결하기 위한 방안을 마련해야 한다.

④ 제3항의 방안에는 다음 각 호의 사항이 포함되어야 한다.

1. 위험 식별, 분석, 평가 등 위험 관리 방안
2. 제품 또는 컴포넌트 패치
3. 제품 보안 문서

⑤ 디지털의료기기제조업자들은 의료서비스제공자에게 안전하게 개인 정보 등을 제거하기 위한 방법을 제공하여야 한다.

제16조(소프트웨어 구성요소 명세서 관리 활동) ① 디지털의료기기제조업자들은 디지털의료기기 내 취약점 발견, 보안 및 침해사고 및 이를 해결하기 위한 활동을 수행하는 데 소프트웨어 구성요소 명세서를 활용할 수 있다.

② 의료서비스제공자는 디지털의료기기에 대해 디지털의료기기제조업자들이 작성한 소프트웨어 구성요소 명세서를 구매 및 설치 이전에 확인하는 것을 고려할 수 있다.

③ 소프트웨어 구성요소 명세서 정보는 보호되어야 하며 소프트웨어 구성요소 명세서의 생성, 저장, 송수신 등의 과정에서 데이터 보안을 고려할 수 있다.

제6장 전자적 침해행위의 대응

제17조(침해행위 대응 계획 등) ① 디지털의료기기제조업자들은 디지털 의료기기 자체 또는 제품을 사용하는 운영 환경을 고려하여 전자적 침해행위에 대응하기 위한 계획을 수립하여야 한다.

② 제1항의 대응 계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 침해행위 신고 방안
2. 침해행위 조치 방안
3. 침해행위 식별, 분석, 평가 등 위험 관리 방안
4. 침해행위 대응팀 구성
5. 제품 사용의 연속성을 보장하기 위한 계획
6. 침해행위 대응을 위한 테스트 및 훈련 방안 등

③ 디지털의료기기제조업자들은 침해행위 발생에 대응하기 위해 대응 인력과 대응 훈련 방안을 마련하여야 한다.

제18조(침해행위 신고) ① 디지털의료기기제조업자들은 디지털의료기기 자체 또는 그 운영 환경에서 전자적 침해행위가 발생한 것을 인지한 경우 이를 즉각 식품의약품안전처장과 의료서비스제공자 및 제품을 이용하는 사용자에게 알려야 한다.

② 의료서비스제공자는 디지털의료기기 자체 또는 그 운영 환경에서 전자적 침해행위가 발생하는 경우 이를 즉각 식품의약품안전처장과 디지털의료기기제조업자들에게 알릴 수 있다.

제19조(침해행위 발생 이후의 조치) ① 디지털의료기기제조업자들은 전

자적 침해행위가 발생한 원인과 대응 방안을 수립된 계획에 따라 조치해야 한다.

② 디지털의료기기제조업자들은 전자적 침해행위의 원인을 분석하고 재발 방지 대책을 수립하고 식품의약품안전처장과 의료서비스제공자에게 이를 알려야 한다.

③ 의료서비스제공자는 전자적 침해행위의 원인 분석 등을 위해 디지털의료기기제조업자들과 협조할 수 있다.

제7장 취약점 감시 및 대응

제20조(취약점 감시) ① 디지털의료기기제조업자들은 디지털의료기기의 취약점 감시를 위해 정기적인 보안 모니터링, 로그 분석 등의 감시 활동을 계획하고 감시, 공개 및 조치 절차에 대해 문서화하여 보관하여야 한다.

② 의료서비스제공자는 디지털의료기기에서 취약점을 확인할 경우 즉시 디지털의료기기제조업자들에게 알릴 수 있다.

③ 디지털의료기기제조업자들은 디지털의료기기에서 취약점을 확인할 경우 즉시 식품의약품안전처장과 의료서비스제공자에게 알릴 수 있다.

④ 디지털의료기기제조업자들은 제3항의 취약점을 식품의약품안전처장에게 알릴 경우 취약점에 대한 상세 내용, 심각도, 영향, 대응 방안 등

을 포함하여야 한다.

⑤ 의료서비스제공자는 보고된 취약점에 대한 분석 및 해결을 위해 디지털의료기기제조업자등이 지원을 요청할 경우 이에 협조할 수 있다.

제21조(취약점 공개) ① 디지털의료기기제조업자등은 제20조제3항의 취약점을 확인할 경우 이를 홈페이지 등에 공개할 수 있다.

② 디지털의료기기제조업자등은 제1항의 취약점 공개 시 보고된 취약점에 대해 상세 내용, 영향, 대응 방안 등을 포함한 자료를 준비하여 홈페이지 등에 공개할 수 있다.

③ 디지털의료기기제조업자등은 취약점에 대해 해결 여부와 심각도 등을 고려하여 공개 시점을 늦출 필요가 있다고 판단될 경우 식품의약품안전처장과 협의를 통해 그 공개 시점을 정할 수 있다.

제22조(취약점 조치) ① 디지털의료기기제조업자등은 보고된 취약점을 해결하기 위한 패치, 업데이트 등의 조치 방안을 마련하여야 한다.

② 디지털의료기기제조업자등 및 의료서비스제공자는 취약점 조치 이후에도 지속적인 모니터링을 통해 취약점이 발생되지 않는지 확인하여야 한다.

제23조(재검토기한) 식품의약품안전처장은 「훈령 예규 등의 발령 및 관리에 관한 규정」에 따라 2025년 1월 1일을 기준으로 매 3년이 되는 시점(매 3년째의 12월 31일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

부 칙

이 고시는 고시한 날부터 시행한다.