의료기기 사이버보안 원칙 및 실무

(Principles and Practices for Medical Device Cybersecurity)

2023. 11.

식품의약품안전처
의 료 기 기 안 전 국

본 문서의 원문(Principles and Practices for Medical Device Cybersecurity)은 전 세계 의료기기 규제당국자들이 자발적으로 구성한 국제의료기기규제당국자포럼(IMDRF)에서 이해당사자 간 협의를 통해 개발되었습니다.

본 문서는 IMDRF에서 발행한 원문을 식품의약품안전처가 알기 쉽게 기술한 것입니다.

본 문서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술방식('~하여야 한다' 등)에도 불구하고 민원인 여러분께서 준수하셔야 하는 사항이 아님을 알려드립니다. 또한, 본 문서는 2023년 11월 현재 과학적·기술적 사실 등을 토대로 작성되었으므로 이후 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

※ 본 문서에 대한 의견이나 문의 사항이 있으면 의료기기안전국 의료기기정책과에 문의하시기 바랍니다.

전화번호: 043-719-3766

팩스번호: 043-719-3750

목 차

1.0 소개

무선, 인터넷 및 네트워크 연결 기기의 사용이 증가함에 따라, 의료기기의 기능과 안전을 보장하기 위한 효과적인 사이버보안의 필요성이 더욱더 중요해졌다. 사이버보안 사고로 인해 의료기기와 병원 네트워크가 작동하지 않아 의료 시설 전반에 걸쳐 환자 진료에 지장이 생기는 경우도 종종 발생하고 있다. 이러한 사고는 진단과 치료 등의 지연 및 오류로 인해 환자의 피해로 이어질 수 있다

의료 분야 내 이해관계자는 의료기기 사이버보안과 관련하여 공동의 책임을 진다. 본 지침의 목적은 미래의 (사이버) 공격, 문제 또는 사건에 대비하여 의료기기를 보호하고 안전하게 유지하는 데 도움이 되는 사전예방적 차원의 사이버보안을 지원하기 위한 각자의 역할을 모든 이해관계자가 더 잘 이해할 수 있도록 교육하는 데 있다.

환자의 안전과 의료기기 성능을 유지하기 위해서는 국제적인 의료기기 사이버보안 원칙과 실무를 통합할 필요가 있다. 그러나 정부별로 상이한 규정으로 인해, 의료기기 사이버보안을 보장하는 데 필요한 국제적인 일관성이 부족한 실정이다.

본 IMDRF 지침 문서의 목적은 의료기기 사이버보안에 관한 국제적 규제의 통합을 촉진하기 위한 일반 원칙 및 모범 실무를 제공하는데 있다. 문서의 구성은 2장에 문서의 범위, 3장에 용어가 정의되어 있다.

4장에서는 의료기기 사이버보안의 일반 원리를 다룬 개요를 제공하고, 5장과 6장에서는 의료기기의 시판 전 및 시판 후 사이버보안 관리의 모범 실무에 관한 사항을 제공한다. 5장에서는 주로 의료기기 제조업체(이하 MDM: Medical Device Manufacturers)를 다루며, 6장에는 모든 이해관계자를 위한 권장사항이 포함되어 있다.

본 문서는 의료기기 사이버보안만을 중점적으로 다룬 첫 IMDRF 지침서이다. 그러나 일반적인 보안 고려사항과 관련하여 유의해야 하는 기타 관련 IMDRF 문서 또한 존재한다. IMDRF/GRRP WG/N47 FINAL:2018은 의료기기와 체외진단의료기기의 설계 및 제조 시 충족해야 하는 통합된 필수 원칙을 제공한다[1]. 본 지침서와 함께 이러한 필수 원칙을 의료기기의 제품 수명 전주기(이하 TPLC : Total Product Life Cycle) 동안 고려해야 한다. IMDRF/SaMD WG/N12 FINAL:2014는 9.3절의 안전 고려사항과 관련하여 정보 보안의 중요성을 설명하고 소프트웨어 의료기기(SaMD)의 정보 보안에 영향을 미치는 몇 가지 특정 요소를 보여준다.

1) N47의 5.8절은 무단 접근으로부터의 보호와 같은 정보 보안 및 사이버보안에 관한 중요한 요구사항을 설명한다. 본 지침서와 함께 이러한 요구사항을 의료기기의 제품수명 전주기(TPLC) 동안 고려해야 한다.

2.0 범위

본 문서는 의료기기(체외진단의료기기 포함) 사이버보안의 일반 원칙 및 모범 실무에 관한 구체적인 권장 사항을 모든 이해관계자에게 제공하기 위해 제작되었다. 본 문서는 MDM, 의료서비스제공자(이하 HCP: HealthCare Providers), 규제기관 및 사용자가 의도된 용도에 따라 기기를 사용하면서 발생할 수 있는 사이버보안 위험을 최소화하고 기기 안전성 및 성능의 유지 관리와 지속성을 보장하기 위한 권장 사항을 간략하게 설명한다. 본 지침의 목적상, HCP에는 의료서비스 제공 조직이 포함된다.

이 문서는 소프트웨어(펌웨어 및 프로그램 가능 논리 제어기(PLC: Programmable Logic Controller)를 포함)를 내장한 의료기기(예: 페이스메이커, 인퓨전 펌프 등)나 소프트웨어 의료기기(이하 SaMD: Software as a Medical Device)에 대한 사이버보안을 고려한다. 대부분의 규제기관이 의료기기의 안전성 및 성능에 대한 권한을 가지고 있으므로, 이 지침의 범위는 환자에게 해를 끼칠 가능성에 대한 고려 사항에 한정된다는 점에 유의해야 한다. 예를 들어, 성능에 영향을 미치거나 임상적 운영에 부정적인 영향을 미치거나 오진단 또는 잘못된 치료를 야기하는 사이버보안 위험이 본 문서의 범위에 해당한다. 개인정보(데이터) 보호 침해와 관련된 문제와 같은 다른 유형의 피해도 중요하지만, 본 문서에서는 다루지 않는다. 또한 본 문서는 MDM 기업 자체의 사이버보안에 대한 중요성을 인정하나, 이는 본 문서의 범위에는 해당하지 않는다. MDM 기업의 보안과 관련된 모범 실무는

NIST의 사이버보안 프레임워크(NIST Cybersecurity Framework)를 참조해야 한다.

본 문서의 목적은 다음과 같다.

- 적절한 사이버보안 보호를 갖춘 의료기기의 설계 및 개발에 위험 기반 접근 방식 채택
- 의료기기 및 연결된 의료 인프라의 안전성, 성능 및 보안 보장
- 사이버보안에 대하여 MDM, HCP, 사용자, 규제기관 및 취약점 발견자를 포함하되 이에 국한되지 않으며, 모든 이해관계자의 공동책임 인식
- TPLC 동안 환자 피해의 위험을 최소화할 수 있도록 이해관계자에게 권장 사항 제공
- 용어를 일관되게 정의하고 의료기기 사이버보안을 달성하기 위한 최신의 모범적 실무 설명
- 사이버보안 사고, 위협 및 취약점에 대비하는 광범위한 정보 공유 정책을 추진하고 투명성을 높이며 대응을 강화

아울러, 의료기기의 유형 및 규제의 차이로 인해 추가적인 고려사항이 필요한 특정 상황이 발생할 수 있다는 점에 유의해야 한다.

3.0 정의

본 문서의 목적상 IMDRF/GRRP WG/N47 FINAL:2018에 제시된 용어와 그 정의는 다음과 같다.

3.1 **자산(Asset)**: 개인, 조직 또는 정부에 가치가 있는 물리적 또는 디지털 개체(ISO/IEC JTC 1/SC 41 N0317, 2017-11-12)

3.2 **공격(Attack)**: 자산을 파괴, 노출, 변경, 비활성화, 도용 또는 자산에 무단으로 접근하려는 시도(ISO/IEC 27000:2018)

3.3 **인증(Authentication)**: 개체에서 주장하는 특성이 옳은지 보증을 제공하는 행위(ISO/IEC 27000:2018)

3.4 **진본성(Authenticity)**: 개체가 자기 자신이라고 주장하는 속성 (ISO/IEC 27000:2018)

3.5 **인가 또는 권한부여(Authorization)**: 데이터 및 기능에 대한 접근 권한 부여를 포함한 권한 부여(ISO 27789:2013)

참고: ISO 7498-2에서 파생된 개념: 접근 권한을 기반으로 하는 접근을 승인하는 권한

3.6 **가용성(Availability)**: 인가된 개체가 필요에 따라 접근가능하고 사용가능한 속성(ISO/IEC 27000:2018)

3.7 **보상적 위험 통제 조치(동의어: 보상 통제)(Compensating Risk Control Measure, Compensating Control)**: 기기 설계의 일부로 구현된 위험 통제 조치 대신(또는 없이) 배치되는 특정 유형의 위험 통제 조치(AAMI TIR97:2019)

참고: 보상적 위험 통제 조치는 영구적이거나 임시적일 수 있다(예: MDM이 추가적인 위험 통제 조치를 포함하는 업데이트를 제공할 수 있을 때까지)

3.8 **기밀성(Confidentiality)**: 권한이 없는 개인, 개체 또는 절차에 정보를 제공하거나 공개하지 않는 속성(ISO/IEC 27000:2018)

3.9 **조정된 취약점 공개(CVD: Coordinated Vulnerability Disclosure)**: 연구자 및 기타 이해관계자가 제조업체와 협력하여 취약점 공개 및 관련 위험을 줄이는데 필요한 해법을 찾는 절차(AAMI TIR97:2019)

참고: 이 절차에는 취약점 및 해결 방법에 대한 정보를 보고, 조정 및 출판하는 등의 작업이 포함된다.

3.10 **사이버보안(Cybersecurity)**: 정보와 시스템이 무단 접근, 사용, 유출, 중단, 수정 또는 파괴와 같은 비인가 활동으로부터 보호되어 기밀성, 무결성, 가용성과 관련된 위험을 수명 주기 전체 동안 수용할 수 있는 수준으로 유지되는 상태(ISO 81001-1:2021)

3.11 **수명 종료 또는 단종(EOL: End of Life)**: 제조업체가 제조업체에서 정한 사용 연수를 초과한 제품을 더 이상 판매하지 않고, 사용자에게 통지하는 절차를 포함한 공식적인 EOL 과정을 진행함으로써 시작되는 제품의 수명 주기 단계

3.12 **지원 종료(EOS)**: 제조업체가 모든 서비스 지원 활동을 종료하고 서비스 지원이 해당 시점을 넘어 연장되지 않아 시작되는 제품의 수명 주기 단계

3.13 **필수 성능(Essential Performance)**: 기본 안전과 관련된 것들 이외의 제조업체가 정한 제한치를 초과하는 손실 또는 저하로 인해 허용할 수 없는 위험을 발생하는 임상적 기능의 성능(IEC 60601-1:2005+AMD1:2012)

3.14 **익스플로잇(Exploit)**: 취약점을 통해 정보 시스템의 보안을 침해하는 정의된 방법(ISO/IEC 27039:2015)

3.15 **무결성(Integrity)**: 데이터가 생성, 전송 또는 저장된 이후 무단으로 변경되지 않은 속성(ISO/IEC 29167- 19:2016)

3.16 **레거시 의료기기 (동의어: 레거시 기기)(Legacy Medical Device, syn. Legacy Device)**: 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 없는 의료기기

3.17 **부인 방지(Non-Repudiation)**: 주장한 사건 또는 조치의 발생 및 해당 원본 개체를 증명할 수 있는 능력(ISO/IEC 27000:2018)

3.18 **환자 피해(Patient Harm)**: 환자의 신체 부상 또는 건강 손상 (ISO/IEC 지침 51:2014에서 수정됨)

3.19 **개인정보 보호(Privacy)**: 해당 개인에 대한 부당하거나 불법적인 데이터 수집 및 사용으로 인해 개인의 사생활이나 일에 대한 침해를 받지 않는 상태(ISO/TS 27799:2009)

3.20 **위협(Threat)**: 보안을 위반하고 피해를 줄 수 있는 상황, 기능, 조치 또는 사건이 있을 때 존재하는 보안 위반 가능성이 있는 상태(ISO/IEC 지침 120)

3.21 **위협 모델링(Threat Modeling)**: 시스템에 피해를 입힐 수 있는 파괴, 공개, 데이터의 수정 또는 서비스 거부 형태의 모든 상황 또는 사건을 노출시키는 탐색적인 과정(ISO/IEC/IEEE 24765-2017에서 적용)

3.22 **업데이트(Update)**: 의료기기 소프트웨어에 대한 수정형, 예방형, 적응형 또는 진보형 수정 사항

참고 1: ISO/IEC 14764:2006에 설명된 소프트웨어 유지 관리 활동에서 파생된 개념

참고 2: 업데이트에는 패치 및 구성 변경 사항이 포함될 수 있다.

참고 3: 적응형 과 진보형 수정 사항은 소프트웨어의 개선 사항이다. 이러한 수정사항은 의료기기의 설계 사양에 포함되지 않았던 수정사항이다.

3.23 **유효성 검사(Validation)**: 객관적인 증거 제공을 통해 의도된 특정 용도 또는 신청(요구사항)을 충족했는지 확인(ISO 9000:2015)

참고 1: “유효성 검사로 확인됨.”이라는 용어는 해당 상태를 나타내는데 사용된다.

참고 2: 유효성 검사의 사용 조건은 실제 또는 시뮬레이션일 수도 있다.

3.24 **검증(Verification)**: 객관적인 증거 제공을 통해 특정 요건이 충족되었는지 확인(ISO/IEC 지침 63)

참고 1: 검증에 필요한 객관적 증거는 검사의 결과일 수도 있고, 대체 계산 수행 또는 문서 검토와 같은 다른 형태의 결과일 수도 있다.

참고 2: 검증을 위해 수행하는 활동은 자격 심사 과정이라고 부르기도 한다.

참고 3: “검증됨“이라는 단어는 해당 상태를 나타내는 데 사용된다.

3.25 **취약점(Vulnerability)**: 하나 이상의 위협에 의해 악용될 수 있는 자산 또는 통제 약점(ISO/IEC 27000:2018)

4.0 일반 원칙

이 장에서는 의료기기의 개발, 규제, 사용 및 모니터링 시 모든 이해관계자가 고려해야 하는 의료기기 사이버보안을 위한 일반지침 원칙을 제공한다. 본 지침서 전체에서 다루고 있는 이 주제는 의료기기 사이버보안의 국제적인 개선에 매우 중요하며, 이러한 원칙을 준수할 경우 환자의 안전에 긍정적인 영향을 미칠 것으로 기대된다.

4.1 국제적인 조화

의료기기 사이버보안은 전 세계적인 관심사다. 보안 사고는 진단 또는 치료의 오류를 야기하거나, 기기의 정상 작동을 저해하거나, 임상적 운영에 영향을 미치거나, 중증 치료를 받으려는 환자의 접근을 막아 전세계 의료 시스템 내 환자의 안전을 위협할 수 있다. 혁신을 장려하고 환자가 안전하고 효과적인 의료기기에 적시에 접근할 수 있도록 함과 동시에 환자의 안전을 유지하기 위해서는 국제적인 의료 사이버보안의 조화를 위해 노력해야 한다. 모든 이해관계자는 의료기기의 수명 주기 전반에 걸쳐 사이버보안에 대한 서로의 접근 방식을 조화롭게 맞추는 것이 좋다. 여기에는 제품 설계 전반의 조화, TPLC 전반에 걸친 위험 관리 활동, 기기 라벨 표시, 인허가 자료 제출 시 요구사항, 정보 공유 및 시판 후 관리 활동이 포함된다.

4.2 TPLC

초기 구상 단계부터 지원 종료(EOS)에 이르기까지 의료기기 수명 주기의 모든 단계에 걸쳐 사이버보안 위협 및 취약점과 관련된 위험을 고려해야 한다. 사이버보안 위험의 역학적 특성을 효과적으로 관리하기 위해서는 TPLC에 걸쳐 위험 관리를 적용해야 한다. 이는 설계, 제조, 테스트 및 시판 후 모니터링 활동을 포함하되 이에 국한되지 않으며, TPLC의 다양한 단계에서의 사이버보안 위험을 평가하고 완화해야 한다.

일반적으로 안전성과 보안의 균형을 맞출 필요가 있다. 사이버보안 통제와 완화 조치를 통합하는 과정에서 MDM이 기기의 안전성 및 필수 성능을 유지하는 작업은 매우 중요하다.

4.3 공동의 책임

의료기기 사이버보안은 MDM, HCP, 사용자, 규제 기관 및 취약점 발견자를 포함한 모든 이해관계자의 공동 책임이다. 모든 이해관계자는 자신의 책임을 이해하고 다른 이해관계자와 긴밀히 협력하며 의료기기의 수명 주기 동안 잠재적인 사이버보안 위험과 위협을 지속해서 모니터링하고, 평가하고, 완화하고, 의사소통하고, 대응해야 한다.

4.4 정보 공유

사이버보안 정보 공유는 안전하고 안심할 수 있는 의료기기를 위한 TPLC 접근 방식의 기본 원칙이다. 모든 이해관계자가 사이버보안 정보를

공유하는 데 있어 사전 예방적 시판 전후 접근 방식을 채택할 것을 권장한다. 적시의 정보 가용성은 모든 담당자가 위협을 식별하고 관련 위험을 평가하며 그에 따라 대응할 수 있도록 향상된 역량을 제공한다. 따라서 모든 담당 이해관계자가 정보 공유 분석 조직(ISAO: Information Sharing Analysis Organizations)에 적극적으로 참여하여 협력을 촉진하고 의료기기 및 연결된 의료 인프라의 안전성, 성능, 무결성 및 보안에 영향을 미칠 수 있는 사이버보안 사고, 위협 및 취약점을 서로 교류할 것을 권장한다. 이러한 노력은 투명성을 촉진한다. 조정된 취약점 공개는 모범 실무로 권장되는 또 다른 정보 공유 메커니즘이다. 그 뿐만 아니라 해당 생태계는 MDM을 넘어 HCP와 사용자까지 포괄하는 정보 공유를 위한 추가적인 정책 개발을 통해 혜택을 얻을 수 있다. 규제 기관도 국제적으로 환자의 안전을 보호하고 유지하는데 도움이 되도록 다른 규제 기관과 정보를 공유하는 것이 좋다.

5.0 의료기기 사이버보안에 관한 시판 전 고려사항

물론 TPLC에 걸쳐 의료기기 사이버보안을 고려해야 하지만, 시판에 앞서 의료기기의 설계 및 개발 중에 MDM이 다루어야 할 중요한 요소가 있다. 이러한 시판 전 요소에는 제품의 보안 기능 설계, 승인된 위험 관리 전략의 적용, 보안 테스트, 사용자가 기기를 안전하게 작동하기 위한 유용한 정보 제공, 시판 후 활동을 위한 계획 수립 등이 있다. 상기 시판 전 요소의 경우, MDM은 의도된 사용 환경과 합리적으로 예측할 수 있는 오용 시나리오를 고려해야 한다. 다음 절의 목적은 TPLC의 시판 전 단계에서 MDM에게 이러한 개념을 소개하고 권장 사항을 제공하는데 있다. 의료기기 소프트웨어의 수명 주기 활동은 IEC 62304:2006/AMD 1:2015에 명시되어 있으니 참고해야 한다.

5.1 보안 요구 사항 및 아키텍처 설계

설계 단계에서 사이버보안 위협을 사전 예방적 차원에서 해결하면 (예: 위협 모델링과 같은 노력을 통해) 시판 후 대응적 차원의 활동에만 참여하는 것보다 환자 피해 가능성을 더욱 낮출 수 있다. 이러한 설계 단계의 입력 정보는 요구 사항 포착, 설계, 검증, 테스트 또는 시판 전후 활동의 위험 관리 활동과 같은 TPLC의 다양한 단계에서 얻을 수 있다.

보안 요구 사항도 수명 주기 설계 절차의 요구 사항 포착 단계에서 확인해야 한다. 일부 보안 요구 사항 및 보안 위험 통제 조치는 AAMI TIR57:2016, IEC TR 80001-2-8, ISO 27000 제품군 및 NIST(예: NIST의

시큐어 소프트웨어 개발 프레임워크(SSDF: Secure Software Development Framework)), 오픈 웹 애플리케이션 보안 프로젝트(OWASP: Open Web Application Security Project)(예: 설계 원칙에 따른 보안), 미국 의료 및 공중 보건 부문 조정 위원회(HPHSCC 또는 HSCC: US Healthcare and Public Health Sector Coordinating Council)의 공동 사이버보안 워킹그룹(JCWG: Joint Cyber Security Working Group)(예: 공동 보안 계획)에서 발행한 문서 등에서 확인할 수 있다.

다음 표 1에서는 전체 목록은 아니지만, MDM이 제품을 설계할 때 고려해야 할 몇 가지 설계 원칙을 간략하게 설명한다.

표 1: 의료기기 설계 시 고려할 엄선된 설계 원칙

설계 원칙	설명
시큐어 통신	MDM은 해당 기기가 다른 기기 또는 네트워크에 접속되는 방법을 고려해야 한다. 접속에는 유선 연결 및/또는 무선 통신이 포함될 수 있다. 접속 방법의 예로는 Wi-Fi, 이더넷, 블루투스(Bluetooth), USB 등이 있다.
	MDM은 모든 입력 정보(외부 입력 정보에 한정하지 않음)의 유효성을 검사하고 보안성이 낮은 통신만 지원하는 기기 및 환경(예: 홈 네트워크에 연결된 기기 또는 레거시 기기)과의 통신을 고려한 설계 기능을 고려해야 한다.
	MDM은 무단 접근·수정·재생을 방지하기 위해 기기 간 데이터 전송 시 보안을 유지하는 방법을 고려해야 한다. 예를 들어, MDM은 기기/시스템 간 통신 시 서로를 인증하는 방법, 암호화 필요 여부, 이전에 전송된 명령 또는 데이터의 무단 재생을 방지하는 방법, 사전 정의된 시간이 지난 후 통신 세션을 종료하는 것이 적절한지 등을 결정해야 한다.
데이터 보호	MDM은 기기에 저장되거나 기기 간 전송되는 안전 관련 데이터에 암호화와 같은 일정 수준의 보호가 필요한지를 고려해야 한다. 예를 들어, 비밀번호를 암호화된 보안 해시로 저장해야 한다.
	MDM은 통신 프로토콜의 메시지 제어/순서 필드를 보호하거나 암호화 키 자료의 손상을 방지하기 위해 기밀성 위험 통제 조치가 필요한지를 고려해야 한다.

기기 무결성	MDM은 데이터 부인 방지(예: 감사 로그 기능 지원)를 보장하기 위한 기능적 설계가 필요한지를 결정하기 위해 시스템 수준의 아키텍처를 평가해야 한다.
	MDM은 해당 기기 소프트웨어에 대한 무단 수정과 같은 기기 무결성을 손상하는 위험을 고려해야 한다.
	MDM은 바이러스, 스파이웨어, 랜섬웨어 및 기타 형태의 악성 코드가 기기에서 실행되는 것을 방지하기 위해 멀웨어 방지와 같은 통제를 고려해야 한다.
사용자 인증	MDM은 기기를 사용할 수 있는 사람의 유효성을 검사하거나 다른 사용자 역할에 권한을 부여하거나 비상시 사용자의 접근을 허용하는 사용자 접근 통제를 고려해야 한다. 또한 동일한 자격 인증서를 기기와 고객 간에 공유해서는 안 된다. 인증 또는 접근 승인의 예로는 암호, 하드웨어 키, 또는 생체 정보 인증 방식 또는 다른 기기에서 만들 수 없는 목적 신호가 있다.
소프트웨어 유지 관리	MDM은 정기적으로 업데이트를 실행하고 배치하기 위한 절차를 수립하고 전달해야 한다.
	MDM은 운영 체제 소프트웨어, 서드파티 소프트웨어 또는 오픈 소스 소프트웨어를 업데이트하거나 통제하는 방법을 고려해야 한다. 또한 MDM은 통제 범위를 벗어난 소프트웨어 업데이트 또는 오래된 운영 환경(예: 보안이 취약한 운영 체제 버전에서 실행되는 의료기기 소프트웨어)에 대응하는 방법을 계획해야 한다.
	MDM은 새로 발견된 사이버보안 취약점으로부터 기기를 보호하기 위해 기기를 업데이트하는 방법을 고려해야 한다. 예를 들어, 업데이트에 사용자 개입이 필요한지 또는 업데이트가 기기에 의해 시작되는지를 비롯해 업데이트가 기기의 안전성 및 성능에 부정적인 영향을 미치지 않는다는 점을 입증할 수 있는 유효성 검사 방법을 고려해야 한다.
	MDM은 업데이트를 수행하기 위해 필요한 연결은 무엇인지와 코드 서명 또는 기타 유사한 방법을 사용하여 연결 또는 업데이트의 진본성을 고려해야 한다.
물리적 접근	MDM은 권한이 없는 사람이 기기에 접근하는 것을 방지하기 위한 통제를 고려해야 한다. 예를 들어, 물리적 잠금 또는 포트에 대한 접근을 물리적으로 제한하거나 인증 요구 없이는 물리적 케이블을 통한 접근을 허용하지 않는 방안을 고려할 수 있다.
신뢰성 및 가용성	MDM은 필수 성능을 보장하기 위해 기기가 사이버보안 공격을 감지하고, 이에 대해 저항, 대응하며 공격으로부터 복구할 수 있는 설계적 기능을 구축해야 한다.

시큐어 개발 원칙은 보안에 안전한 기기 설계에 필수적이다. 현재의 소프트웨어 개발 수명 주기 모델 또는 표준에는 이러한 원칙이 기본 원칙으로 정립되어 있지 않다. 의료기기 소프트웨어를 개발하는 MDM은 소프트웨어 개발 과정에 이러한 보안 원칙을 통합하는 것이 중요하다. 이렇게 하려면 MDM이 TPLC 전반에 걸쳐 위험과 완화 요소를 평가함으로써 기기 사이버보안에 대한 통합적인 접근 방식을 취해야 한다.

5.2 TPLC 위험 관리 원칙

의료기기의 수명 주기 전체에 걸쳐 보안 및 안전 영역을 다루는 확고한 위험 관리 원칙을 통합하여야 한다. 기기 안전 및 필수 성능에 영향을 미치거나, 임상 실무에 부정적인 영향을 주거나 오진단 또는 잘못된 치료를 야기하는 사이버보안 위험도 의료기기의 위험 관리 절차에서 고려해야 한다. MDM은 ISO 14971:2019에 설명된 위험 관리 및 사이버보안 위험 관리(예: AAMI TIR57:2016; AAMI TIR97:2019에서 설명된 바와 같이)를 사용하여 위험 관리 절차의 일환으로 다음 단계를 수행해야 한다.

- 사이버보안 취약점 파악
- 관련 위험 추정 및 평가
- 해당 위험을 허용할 수 있는 수준으로 통제
- 위험 통제 효과 평가 및 모니터링
- 조정을 거쳐 주요 이해관계자에게 위험 정보를 전달

아래 그림 1은 AAMI TIR57:2016의 보안 위험 관리 절차를 보여준다. 이는 전체 위험 관리의 일부로 수행되는 특별한 위기관리 절차에 해당하거나, 취약점, 위협 및 기타 보안 관련 용어의 적절한 매핑과 함께 ISO 14971:2019 위험 관리 절차의 필수적인 부분으로 간주할 수 있다. 가능한 매핑에 관한 정보는 ISO/TR 24971:2020 부록 F를 참조하면 좋다.

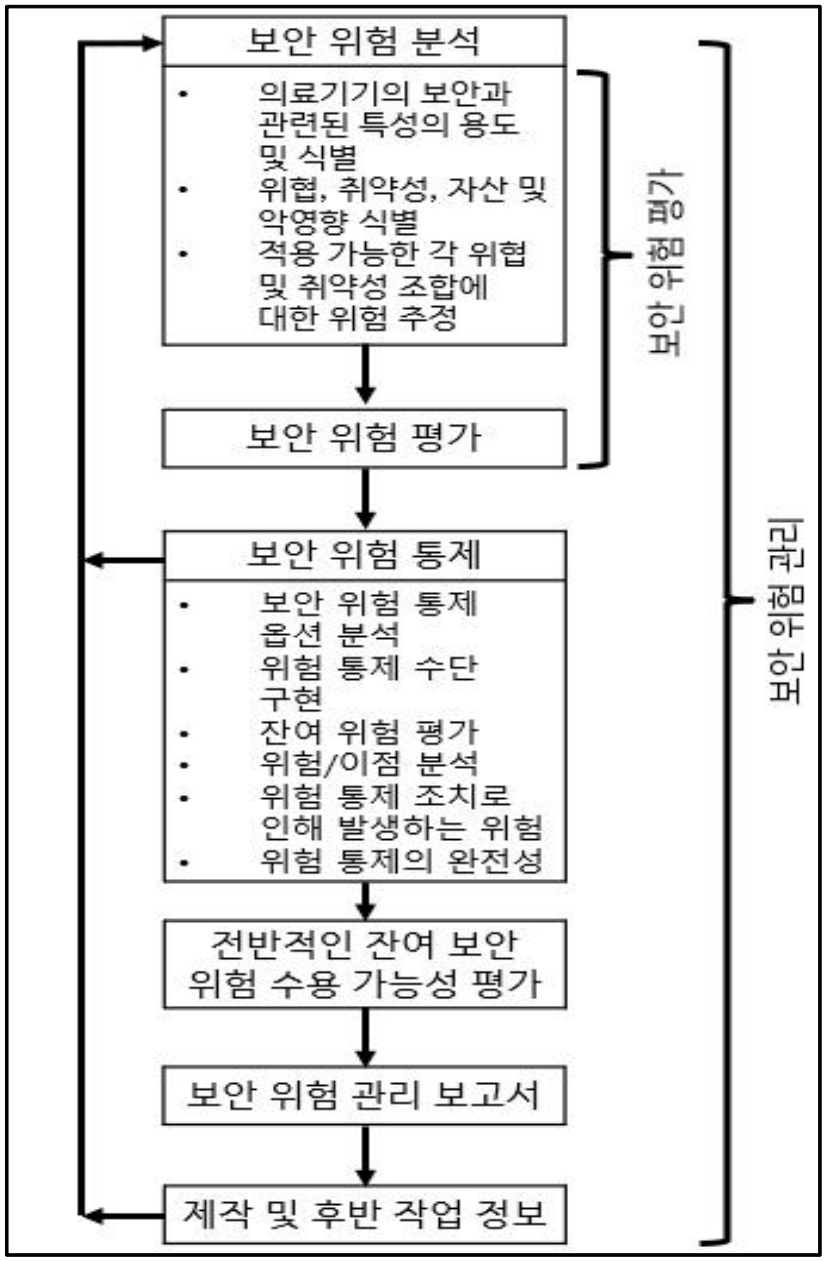

그림 1: 보안 위험 관리 절차의 도식화
(AAMI TIR57:2016 승인)

의료기기 규정의 사이버보안 측면에서 위험 분석은 다음을 고려하여 환자 피해 위험을 평가하는 데 중점을 두어야 한다. 1) 사이버보안 취약점 공격 가능성, 2) 취약점을 공격할 경우, 환자 피해의 심각성 및 이러한 분석 수행 시 보상적 통제 및 위험 완화 조치도 고려해야 한다.

위험 평가는 설계와 위협 모델링, 환자 피해, 완화, 테스트를 연계한다. 따라서 이러한 위험을 적절히 관리할 수 있도록 시큐어 설계 아키텍처를 수립하는 것이 중요하다. 이러한 평가 수행 시 보안 위험 평가, 위협 모델링 및 취약점 점수 평가를 포함하되 이에 국한되지 않는 다양한 도구와 접근 방식을 활용할 수 있다.

- **보안 위험 평가**: MDM은 TPLC 전반에 걸쳐 사이버보안 위험, 위협 및 통제를 고려해야 한다. 해당 요구 사항이 식별된 위험에 대한 완화 요소라면, 해당하는 경우, 사이버보안 요구 사항을 특정 기기 사이버 보안 위협 및 취약점과 상호 참조해야 한다.

- **위협 모델링**: 위협 모델링은 기기와 시스템의 잠재적 위협으로부터 위험을 식별, 열거 및 완화하기 위한 절차이다. 위협 모델링에는 특수 공급망(예: 시스템 컴포넌트), 설계, 생산, 배치(예: 병원 환경에) 및 유지 관리와 관련된 위험을 포함하되 이에 국한되지 않는 위험 요소를 고려해야 한다. 충분히 상세한 시스템 다이어그램을 제작하면 사이버보안 설계 요소가 어떻게 기기에 통합되어 해당 기기로 위협 모델링을 보다 효과적으로 지원하는 방법을 이해하는 데 도움이 된다. MDM은 위협 모델을 생성하는 데 OWASP의 지침에 따라 사이버 보안과 관련된 4가지 기본 질문에 답해야 한다.

  1. 구축하는 모델은 무엇인가?
  2. 잠재적 문제는 무엇인가?(예: 가능한 공격 방법)

3. 이러한 부분에 어떤 조치를 취할 것인가?
4. 충분한 조치를 취했는가?

애플리케이션 아키텍처, 운영 데이터 흐름 또는 더 광범위한 시스템 수준의 위협 모델링 상황에서 해당하는 경우 위와 같은 질문을 통해 상황을 파악할 수 있다. 위협 모델링 중에 무엇이 잘못될 수 있는지를 파악할 때 MDM은 소프트웨어 및 하드웨어의 의도하지 않거나 악의적인 잘못된 구성(예: 인터넷 연결용으로 설계되지 않은 기기를 연결하는 경우)을 고려해야 한다.

- **취약점 점수 매기기**: 취약점 점수 매기기는 사이버보안 취약점에 대한 공격 가능성 및 취약점의 심각성을 특성화하고 평가하는 방법을 제공한다. 설계 및 개발 시 식별된 알려진 공통 취약점 및 노출(CVE: Common Vulnerabilities and Exposures)은 공통 취약점 점수 시스템(CVSS: Common Vulnerability Scoring System) 또는 향후에 널리 채택될 취약점 점수 시스템과 같은 일관된 취약점 점수 매기기 방법론을 사용하여 분석 및 평가해야 한다. 사이버보안 위험, 취약점 점수 매기기 및 통제 조치를 사용하여 사이버보안에만 특화되지 않은 신제품 및 기타 위험 평가 도구(예: 고장 모드 및 효과 분석(FMEA: Failure Mode and Effects Analysis))에 위협 모델링 및 보안 위험 평가 정보를 제공할 수 있다.

보안 위험 관리 절차를 기존 ISO 14971:2019 위험 관리 절차에 통합

할 때 위협 모델링 및 취약점 점수 매기기와 같은 보안을 다루는 활동을 고려해야 한다.

5.3 보안 테스트

MDM은 설계 및 개발 절차의 검증 및 유효성 검사 단계에서 해당 코드에 알려진 중요한 취약점이 없고 보안 통제가 효과적으로 실행되었음을 보장하기 위해 다양한 보안 테스트를 실시해야 한다. 이러한 테스트를 진행할 때는 해당 기기의 사용 상황과 배치 환경을 고려해야 한다. 소프트웨어가 사양을 준수하도록 하고 이상 현상을 최소화하려면 소프트웨어 검증 기법을 적용하는 것이 좋다. 또한 알려진 취약점에 대해 의료기기를 테스트하는 것도 중요하다. 이를 위해서는 해당 의료기기가 보안 평가 절차 또는 승인 검사(예: 소프트웨어 테스트, 공격 시뮬레이션 등)를 받아야 한다. 보안 테스트는 시큐어 개발 프레임워크의 컴포넌트이다. 테스트 고려 사항에 관한 추가 상세 정보는 5.1절에서 제공되는 표준 및 자원에서 확인할 수 있다. MDM을 위한 몇 가지 높은 수준의 고려사항은 다음과 같다.

- 개발 중에 알려진 취약점 또는 소프트웨어 약점에 대해 소프트웨어 컴포넌트/모듈에서 대상 검색을 수행한다. 예를 들어, 정기적인 보안 테스트에는 정적 코드 분석, 동적 분석, 견고성 테스트, 취약점 검사 또는 소프트웨어 구성 분석이 포함될 수 있다.
- 기술적 보안성 분석(예: 침투 테스트)를 수행한다. 예를 들어, 여기에는 퍼즈(Fuzz) 테스트를 통해 알려지지 않은 취약점을 식별하거나

대체 진입점(예를들면, 숨겨진 파일, 구성(Configuration), 데이터 스트림 또는 하드웨어 레지스터를 읽음으로 해서 찾아낸 대체진입점)을 검사하는 작업이 포함된다.

- 취약점 평가를 완료한다. 여기에는 다른 내부 제품에 취약점이 미친 영향을 분석하고(즉, 변이 분석), 대책을 식별하며, 취약점을 개선 또는 완화하려는 작업이 포함된다.

5.4 TPLC 사이버보안 관리 계획

사이버보안 위협이 지속해서 발전함에 따라, TPLC에 걸쳐 사이버보안 관리 계획의 일환으로 사전 예방적 차원에서 취약점과 취약점에 대한 공격을 모니터링, 식별, 해결해야 하는 MDM의 책임이 중요해졌다. 제품 개발의 시판 전 단계에서 계획을 진행해야 하며, 가장 이상적으로는 MDM의 조직 전반에 걸쳐 해당 계획을 유지해야 한다. 이 계획에는 다음을 다루어야 한다.

- **TPLC 감시**: 새로 발견된 사이버보안 취약점을 사전 예방적 차원에서 모니터링 및 식별하고, 위협을 평가하고, 적절하게 대응
- **취약점 공개**: 취약점 발견자로부터 정보를 수집하고, 완화 및 개선 전략을 개발하며, 취약점의 존재와 완화 또는 개선 접근 방식을 이해관계자에게 공개하기 위한 공식화된 절차
- **업데이트 및 개선**: 정기적으로 또는 식별된 취약점에 대한 대응으로 기기의 지속적인 안전성 및 성능을 유지하기 위해 소프트웨어를 업데이트하는 방법 또는 기타 개선 조치를 적용하는 방법을 간략히 설명하는 계획

- **복구**: 사이버보안 사고 이후 MDM, 사용자 또는 양쪽 모두가 기기를 정상 작동 상태로 되돌리기 위한 복구 계획
- **정보 공유**: 보안 위협 및 취약점 관련 업데이트된 정보의 전달 및 공유를 촉진하는 정보 공유 분석 조직(ISAO: Information Sharing Analysis Organizations) 또는 정보 공유 및 분석 센터(ISAC: Information Sharing and Analysis Centers)에 참여

5.5 라벨 표시 및 고객 보안 문서

5.5.1 라벨 표시

라벨 표시는 상대적인 사이버보안 위험을 고려하여 최종 사용자에게 관련 보안 정보를 전달한다. 다음 요소를 포함해야 한다.

- 의도된 사용 환경(예: 멀웨어 방지 소프트웨어, 네트워크 연결 구성, 방화벽 사용)에 적합한 권장 사이버보안 통제와 관련된 기기 지침 및 제품 사양
- 백업 및 복원 기능과 구성 복원 절차에 관한 설명
- 데이터를 수신 및/또는 송신할 것으로 예상되는 네트워크 포트 및 기타 접속의 목록과 포트 기능 및 포트의 수신 또는 송신 여부에 관한 설명(사용하지 않는 포트는 비활성화해야 함.)
- 최종 사용자를 위한 충분히 상세한 시스템 다이어그램

5.5.2 고객 보안 문서

사용 지침 외에도 기기의 설치, 구성을 위해 MDM이 작성한 기술 문서와 작동 환경에 대한 기술 요구 사항은 사용자가 기기를 안심하고 안전히 사용하는데 특히 중요하다. 다음 요소를 포함해야 한다.

- 기기를 의도한 대로 작동할 수 있도록 지원 인프라 요구 사항에 관한 명확한 사용자 지침
- 보안에 안전한 구성을 사용하여 기기의 보안을 강화하거나 강화할 수 있는 방법에 관한 설명. 보안에 안전한 구성에는 멀웨어 방지, 방화벽/방화벽 규칙, 화이트리스트, 보안 사건 매개 변수, 로깅 매개 변수, 물리적 보안 감지 등과 같은 엔드포인트 보호 기능 포함될 수 있다.
- 해당하는 경우, 시큐어 네트워크(연결형) 및 서비스를 허용하는 기술 지침과 사이버보안 취약점 또는 사고 감지 시 대응 방법에 관한 사용자 지침
- 이상 상황(예: 보안 사건) 감지 시, 가능한 경우에 기기 또는 지원 시스템이 이를 사용자에게 알리는 방법에 관한 설명. 보안 사건 유형에는 구성 변경, 네트워크 이상 현상, 로그인 시도, 이상 트래픽(예: 알 수 없는 개체에 요청 송신) 등이 있다.
- 권한이 있는 인증된 사용자가 기기 구성을 보존 및 복구하는 방법에 관한 설명
- 해당하는 경우, 보안 구성 또는 사용 환경의 변경으로 인한 보안 위험 및 결과, 인증된 사용자가 MDM이 제공한 업데이트를 다운로드 및 설치할 수 있는 체계적인 절차에 관한 설명

- 알려진 경우, 기기 사이버보안 지원 종료와 관련된 정보(6.6절, 레거시 의료기기 참조)
- 의료기기에 포함된 상업용, 오픈 소스 또는 상용(OTS: Off-The-Shelf) 소프트웨어 컴포넌트의 사이버보안에 관해 운영자에게 알리고 지원하는 소프트웨어 자재 명세서(SBOM : Software Bill of Materials)는 이름, 출처, 버전 및 빌드에 따라 각 소프트웨어 컴포넌트를 식별하는 목록을 통해 요구되는 투명성을 제공한다. SBOM을 사용하면 기기 운영자(환자 및 HCP 포함)는 자산 및 관련 위험을 효과적으로 관리하고, 식별된 취약점이 기기(및 연결된 시스템)에 미치는 잠재적 영향을 이해하고, 기기의 안전성 및 필수 성능을 유지하기 위한 대책을 마련할 수 있다. 기기 운영자는 SBOM을 통해 MDM과 더욱 협력하여 취약점 및 업데이트 요구 사항이 있을 수 있는 소프트웨어를 식별하고, 적합한 보안 위험 관리를 수행할 수 있다. 또한 SBOM은 잠재 구매자에게 애플리케이션에 사용되는 컴포넌트에 대한 가시성을 제공하고 잠재적인 보안 위험을 판단하여 구매 결정을 내리는 데 필요한 정보를 제공한다. MDM은 SBOM에 사용되는 형식, 문법, 마크업의 업계 모범 실무를 활용해야 한다. SBOM은 의료기기의 민감한 정보를 공개하기 때문에 신뢰할 수 있는 통신 채널을 통해 배치하는 것이 좋다. 일반적으로 MDM이 운영자에게 SBOM을 전달하는 신뢰할 수 있는 방법을 결정한다.

5.6 규제 제출용 문서

MDM은 앞선 장에서 설명한 활동 외에도 사이버보안과 관련된 활동을

명확하게 문서화하고 요약해야 한다. 규제 기관은 기기의 위험 등급에 따라 의료기기를 평가하기 위해 이러한 유형의 문서를 시판 전 또는 TPLC의 시판 후 단계에서 요구할 수 있다. 시판 전 승인을 위해 필요한 경우, MDM은 기기의 설계 기능, 위험 관리 활동, 테스트, 라벨 표시를 비롯해 TPLC에 걸쳐 새로 등장한 사이버보안 관련 위협을 모니터링하고 대응하기 위한 계획의 증거를 설명하는 명확한 문서를 제출해야 한다. 다음 단락에서는 위의 각 항목에 관한 자세한 내용을 제공한다.

5.6.1 설계 문서

접속 또는 통신 경로 또는 컴포넌트(하드웨어 및 소프트웨어), 그리고 위의 5.1절에서 앞서 약술한 바와 같은 환자 피해와 관련된 사이버보안 위험을 완화하기 위해 포함된 모든 설계 기능(특히 접근 통제, 암호화, 시큐어 업데이트, 로깅, 물리적 보안 등에 대한 조치를 선택하게 된 근거와 가정)을 포함하여 기기를 설명하는 문서이다.

5.6.2 위험 관리 문서

사이버보안 위협과 취약점, 관련 위험의 추정, 그러한 위험을 완화하기 위해 시행하고 있는 통제에 관한 설명, 이러한 통제를 적절하게 테스트했음을 입증하는 증거를 명확하게 설명하는 문서이다. MDM은 다른 안전 통제에 지나치게 영향을 미치지 않는 선에서 기기의 사이버보안을 극대화하는 위험 통제를 고려해야 한다. 특히 규제 기관에 제출하는 사이버보안 관련 위험 관리 문서는 명확해야 하고, 지침을 위해 사이버

보안 위험 관리 표준(예: AAMI TIR57:2016, AAMI TIR97:2019)을 사용해야 한다. 출력물을 전반적인 위험 관리를 위한 입력물로 사용할 수 있도록 해당 결과가 ISO 14971:2019의 전반적인 요구 사항과 일치해야 한다. 사이버보안 관련 위험 관리 문서에는 다음이 포함될 수 있다.

- 위협 모델링 및 식별된 사이버보안 위협이 포함되어 있어야 하는 위험 관리 보고서 또는 보안 위험 관리 보고서와 같은 포괄적인 위험 관리 문서
- 보안 위험 완화가 다른 위험 관리에 미치는 영향에 관한 논의

5.6.3 보안 테스트 문서

기기의 보안 및 보안 통제의 효과를 확인하기 위해 수행한 모든 테스트를 요약한 테스트 보고서이다. 예를 들어, 알려진 취약점 데이터베이스와 소프트웨어 컴포넌트 또는 하위 시스템을 상호 참조하는 등 특정 테스트에 관한 자세한 내용은 위 5.3절에서 확인할 수 있다. 모든 테스트 문서는 다음을 포함해야 한다.

- 테스트 방법, 결과, 결론에 관한 설명
- 보안 위험, 보안 통제, 해당 통제를 검증하기 위한 테스트 간의 추적성 매트릭스
- 사용된 모든 표준 및 내부 SOP 문서에 관한 참고 문헌

5.6.4 TPLC 사이버보안 관리 계획 문서

MDM이 TPLC에 걸쳐 기기의 지속적인 안전성과 성능을 보장하기

위한 시판 후 절차를 설명하는 기기 유지 관리 계획을 요약한 문서이다. 위 5.4절에서 설명된 바와 같이, 이러한 계획된 절차에는 TPLC 감시, 계획된 업데이트 또는 수정 업데이트, 조정된 취약점 공개 정책, 정보 공유가 포함될 수 있다.

5.6.5 라벨 표시 및 고객 보안 문서

사용자가 기기의 의도된 환경에서 위험을 효과적으로 관리할 수 있도록 하기 위해 5.5절에 약술된 대로 관련 정보를 포함하는 모든 사용자 문서이다.

6.0 의료기기 사이버보안에 관한 시판 후 고려사항

취약점은 시시각각 새롭게 발견된다. 그렇기 때문에 이미 설계가 완료되고 실행된 시판 전 통제는 허용할 수 있는 위험 프로파일을 유지하기에 부족할 수 있으므로, 여러 이해관계자가 역할을 수행하는 시판 후 접근 방식이 필요하다. 이 시판 후 접근 방식에는 의도된 환경에서 기기 작동, 정보 공유, 조정된 취약점 공개, 취약점 개선, 사고 대응, 레거시 기기가 포함된다. 다음 절의 목적은 TPLC의 시판 전 단계에서 모든 주요 이해관계자에게 이러한 개념을 소개하고 권장 사항을 제공하는 데 있다.

6.1 의도된 사용 환경에서의 기기 작동

6.1.1 HCP 및 환자

a. HCP가 채택해야 할 사이버보안 모범 실무

의료기기 사이버보안은 공동의 책임이며 HCP를 포함한 모든 이해관계자의 참여가 필요하다. HCP는 IT 인프라에 연결된 의료기기의 안전성, 성능 및 사이버보안 측면을 해결하기 위한 위험관리 절차의 채택을 고려해야 한다. 다음의 경우 위험 관리 절차가 적용되어야 한다.

- IT 인프라의 초기 개발 단계
- 새로운 의료기기를 기존 IT 네트워크에 통합하는 경우
- 운영 체제 또는 IT 네트워크의 변경이나 업데이트 또는 수정을 동반한

의료기기 자체(소프트웨어 및 펌웨어)의 변경이 있는 경우

위에서 언급한 위험 관리 절차를 수행하기 위해 HCP는 IEC 80001-1, ISO 31000 및 ISO 27000 일련 문서를 참조하거나, ISO 27799와 같은 관련 표준을 참조할 수 있다. 의료 산업 사이버보안 실무: 위협 관리 및 환자 보호(The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients) 문서도 참고할 수 있다.

위험 관리 시스템을 채택하는 것 외에도, HCP는 HCP의 전반적인 보안 상태를 유지하기 위해 다음과 같은 일반적인 사이버보안 모범 실무(전체 목록은 아님)를 준수해야 한다.

- 의료기기 또는 네트워크 액세스 포인트(AP)에 대한 무단 물리적 접근 방지를 위한 충분한 수준의 물리적 보안
- 권한이 있는 인력만이 네트워크 요소, 저장된 정보, 서비스 및 애플리케이션에 대한 접근이 가능하게 하기 위한 접근 통제 조치(예: 역할 기반)
- 현재의 모든 자산을 식별하고 향후 구성 변경을 추적하기 위한 구성 관리 사용
- MDM이 권장하는 구성 및 보호 조치 적용
- 의료기기 통신을 제한하기 위한 네트워크 접근 통제
- 적시에 보안 업데이트가 진행되도록 하는 업데이트 관리 실무
- 공격을 방지하기 위한 멀웨어 보호 기능 제공
- 장시간 방치된 기기에 대한 무단 접근을 방지하기 위한 세션 제한 시간 설정

이러한 모범 실무는 기기의 임상적 사용 맥락에서 실행되어야 한다. 예를 들어, 의료 응급 상황에서는 이러한 모범 실무 중 일부를 준수하지 못할 수 있다. 위의 많은 실무는 NIST 사이버보안 프레임워크에 설명되어 있다.

b. 모든 사용자를 위한 훈련/교육

마지막으로, HCP는 자신의 기관에서 사이버보안 사고가 발생하지 않도록 전체적인 접근 방식을 취해야 한다. 따라서 HCP는 보안 인식을 제고하고 모든 사용자(예: 의사, 간호사, 생체의학 엔지니어, 기술자 등)에게 사이버 위생 실무를 소개하기 위한 기본적인 사이버보안 교육을 제공하는 것이 좋다. 여기에는 의료기기를 보안에 안전한 방식으로 작동하는 방법(예: 기기를 보안 네트워크에 연결하는 방법)과 비정상적인 기기 동작(예: 무작위 종료/재시작, 보안 소프트웨어 비활성화)을 발견하고 보고하는 방법에 관한 교육이 포함된다. 또한 환자가 직접 작동하도록 설계된 연결된 의료기기(예: 연속 혈당 모니터 또는 휴대용 인슐린 펌프와 같은 가정용 기기)의 경우, 이러한 훈련을 해당 환자에게도 확대 적용해야 한다.

6.1.2 MDM

제품 라벨 표시 및 고객 보안 문서에 포함된 정보 외에도, MDM은 기기의 최적 배치 및 구성을 보장하기 위해 가능한 경우 HCP, 유통업자, 제품 소비자와 협력하는 것이 좋다.

6.2 정보 공유

정보 공유는 세계 경제의 여러 분야에 걸쳐 사이버보안 위협 및 취약점을 관리하기 위한 필수 도구이다. 보안 인텔리전스 및 위협 공유에 관한 표준과 모범 실무가 의료 분야 이외의 분야에서 개발되고 실행되고 있다. IMDRF에서는 의료기기 이해관계자가 전 세계적으로 의료기기 생태계의 보안을 강화하기 위해 다른 분야에서 이미 입증된 도구를 채택하는 것을 권장한다.

이해관계자에 따라 자원에 대한 접근, 방법, 성숙도 수준이 다양하기 때문에 정보 공유에 대한 유효한 접근 방식의 범위도 다양하다. 게다가 사이버보안 모범 실무는 지속해서 발전하고 있으며, 의료기기 유형, 연결된 인프라, 조직 규모 및 성숙도, 위협 수준을 포함한 여러 요소를 통한 정보도 축적되고 있다. 따라서 본 문서에서는 특정 접근 방식을 다른 접근 방식보다 우위에 놓지 않는다. 대신, 정보 공유와 관련하여 지켜야 하는 원칙은 명확히 설명한다. 예시는 요구 사항을 명시하기 위한 것이 아니라 설명하기 위해 사용된 것이다.

6.2.1 주요 원칙

- 의료기기의 보안과 관련된 정보는 논의 중인 의료기기가 안전하게 사용될 수 있도록 하기 위하여 해당 정보가 필요한 모든 사람(예: 사용자, 환자, 기타 MDM, 유통업자, HCP, 보안 연구원, 일반 대중)에게 공유되어야 한다.

- 공유 정보는 균형을 이루어 다양한 이해관계자에게 의미 있고, 소비할 수 있으며, 조치할 수 있는 정보(예: 보다 보안에 안전한 칩셋에 관한 정보는 MDM에게 중요할 수 있지만, 기기의 최종 사용자에게는 어떠한 이점도 제공하지 않을 수 있음)여야 한다.
- 정보는 상업적 이익과 관계없이 환자의 안전을 개선하고자 하는 목적으로 제한 없이, 선의에 따라 적절한 방식으로 공유되어야 한다.
- 다양한 관할 구역의 이해관계자가 그에 따라 적절히 대응할 수 있도록 여러 관할 구역에서 실시간으로 공유되는(해당하는 경우) 가능한 많은 일관된 국제적인 정보를 보장해야 한다.

6.2.2 주요 이해관계자

의료기기 분야는 세계적인 분야이며, 또한 규제를 받고 있다. 그 결과, 여러 시장에 기기를 공급하는 MDM 입장에서는 지역 또는 관할 구역의 정보 공유 권장 사항만으로는 충분하지 않을 수 있다. 의료기기의 보안과 관련된 정보 공유 전략은 국제적이어야 한다. 그러므로 이해관계자는 일부 네트워크가 국제적일 수 있다는 점을 인식해야 하며, 여러 네트워크에 참여해야 할 수도 있다.

a. 규제 기관

- 의료기기 보안 관련 정보의 주요 수신자이며 정보 보급에 자주 관여한다.
- 의료기기의 사이버보안과 관련된 정보를 적시에 공개하도록 권장하는 절차의 구축을 목표로 한다. 이러한 정보 공개에는 전 세계적으로

조정된 대응을 촉진하기 위한 규제 기관 간의 정보 공유가 포함되어 있다.

b. MDM

- 정보의 출처와 관계없이 취약점 정보를 식별, 평가, 공유해야 한다. MDM은 규제 기관의 기대치를 관리하고 규제 요구 사항이 용이하게 하는 데 도움이 되는 모든 정보를 공유하는 것이 좋다.
- 규제 대상 제품이 배치되는 모든 규제 기관의 통지를 실시간으로 동기화하여 전 세계적으로 일관된 정보를 제공하고, 해당하는 경우, 전 세계적으로 일치하는 대응할 수 있도록 하는 것을 목표로 해야 한다.
- 의료기기 사이버보안 취약점 및 위협과 관련하여 조치할 수 있는 정보를 전달하기 위해서, 의도된 사용자에게 맞는 적절한 수준의 이해하기 쉬운 언어를 사용해야 한다. 여기에는 업데이트가 제공될 때까지 업데이트 배치 또는 보상적 통제와 관련된 임상적 이점과 위험에 관한 정보가 포함될 수 있다.

c. HCP

- 대부분 조치를 취하거나 조치를 용이하게 하는 업무를 담당한다. 그러므로 권장 사항을 실행하고 환자를 보호하는 데 필요한 모든 정보에 접근할 수 있어야 한다.
- 또한 현장에서 의료기기와 함께 작업하고 실제 환경에서 개선 조치 또는 완화를 실행하는 데 있어 용이성/효율성 뿐만 아니라 영향을 받은 기기에 관한 피드백을 제공할 수 있기 때문에 정보의 주요 생성자이다.

d. 사용자(예: 임상의, 환자, 간병인, 소비자)

- 업데이트 또는 기타 수정 작업 조치를 취할지 여부를 최종적으로 결정하는 경우가 많다. 그러므로, 정보에 입각한 결정을 내릴 수 있도록 명확하고 의미 있는 정보가 필요하다.

e. 정부 및 정보 공유 개체를 포함한 기타 이해관계자

- 법 집행 기관, 국가 보안 및 기타 정부 기관은 의료 및 기타 중요한 인프라를 보호하기 위해 의료기기 사이버보안 위협 및 취약점 정보를 여러 정부 부처 간에 공유해야 할 수 있다.
- 정보를 수집 또는 공유하거나 보안 자문 또는 전문 지식을 제공하는 개체도 지원 자원뿐만 아니라 중요한 보안 정보 출처가 될 수 있다. 이러한 단체는 정부 또는 민간 단체일 수 있다. 예로는 정보 공유 네트워크(예: ISAO, ISAC), 보급 기관(예: 컴퓨터 비상 대응 팀(CERT: Computer Emergency Response Teams) 등이 있다. 이러한 이해관계자는 관할 구역과 시장에 따라 다를 수 있다.

6.2.3 정보의 유형

사이버보안 취약점은 소프트웨어 및 하드웨어를 포함한 여러 제품 컴포넌트와 자사 또는 서드파티 컴포넌트에 위협을 줄 수 있다. 환자를 피해로부터 보호하기 위해 공유 정보에는 다음이 포함될 수 있지만 이에 국한되지는 않는다.

- 취약점의 영향을 받는 제품 및 제품이 어떻게 영향을 받는지에 관한 정보
- 다른 제품에서 사용되는 컴포넌트의 취약점에 관한 정보
- 의료기기의 보안에 영향을 미칠 수 있는 IT 장비에 관한 정보
- 공격, 잠재적인 공격 및 취약점 공격 코드의 가용성에 관한 정보
- 사고 확인(예: “같은 문제가 발생하는가?”)
- 패치 및 보상적 통제와 같은 기타 보안 완화 기능의 가용성
- 임시 조치로서 의료기기의 사용 및 통합에 관한 추가 지침

또한 정보 공유에는 위협을 완화할 수 있는 방법, 예를 들어 의료기기에 영향을 미치는 취약점을 완화하도록 IT 장비를 구성하는 방법 또는 알려진 취약점 공격에 대응하는 방법이 포함되어야 한다.

6.2.4 신뢰할 수 있는 의사소통

보안 및 환자 안전을 개선하기 위해 정보를 공유하고, 공유된 정보를 상업적 이익을 얻기 위해 사용해서는 안 된다는 이해와 서면 합의를 통해 정보 공유 네트워크를 구축해야 한다. 정보 공유를 권장하는 한 가지 방법은 익명으로 정보를 공유하는 것이다.

6.3 조정된 취약점 공개(CVD)

알려지지 않은 정보를 확보하는 것이 어렵기 때문에 투명성은 사이버 보안의 필수 컴포넌트이다. 투명성을 향상하는 한 가지 메커니즘은

조정된 취약점 공개(CVD)이다. CVD는 사이버보안 취약점 정보를 획득하고, 취약점을 평가하며, 완화 및 보상적 통제를 개발하고, 고객, 같은 업계 회사, 정부 규제 기관, 사이버보안 정보 공유 조직 및 일반 대중을 포함한 다양한 이해 관계자에게 해당 정보를 공개하기 위한 공식화된 절차를 수립한다.

CVD 정책 및 절차의 채택은 영향을 받는 기술의 최종 사용자가 의료기기, 의료 IT 인프라 및 환자를 더 잘 보호하기 위해 취할 수 있는 조치와 관련하여 더 많은 정보에 입각한 결정을 내릴 수 있도록 지원하는 사전 예방적 접근 방식이다.

CVD에 참여하는 일은 보안 문제에 대한 인식을 제고하기 위한 책임 있는 조치이며, 다른 산업 분야에서 언급된 바와 같이 지속적인 품질 향상 및 위험 관리와 관련된 MDM의 성숙도의 표시로 간주해야 한다.

CVD에 대한 전향적인 입장은 사전 예방적 차원의 책임 있는 기업 행동의 한 사례이지만, 이러한 모범 실무를 채택한 결과 MDM이 부정적인 여론에 직면하게 된 불운한 사례가 몇 차례 있었다. 모범 실무로서의 CVD는 예외가 아닌 표준으로 삼아야 하며, 의료기기 이해관계자는 MDM에게 CVD 정책을 문의하여 채택을 촉진하는 것이 좋다.

6.3.1 MDM

의료기기 생태계가 계속 성숙해짐에 따라 투명한 방식으로 행동해서 얻을 수 있는 이점이 더욱 충분히 인식될 것이다. 이러한 유형의 공개는

동일한 취약점의 영향을 받을 수 있는 여러 시판 제품의 잠재적 피해로부터 대중을 선제적으로 보호하기 때문에 매우 중요하다. 또한 신제품의 보안 설계를 개선할 수 있기 때문에 MDM은 투명한 방식의 행동을 통해 직접적인 혜택을 보게 된다. HCP 및 환자는 MDM과 CERT, 컴퓨터 보안 사고 대응 팀(CSIRT: Computer Security Incident Response Teams) 또는 정부 규제 기관과 같은 컴퓨터 대응팀의 CVD가 취약점과 관련된 권위 있는 정보 출처임을 인식해야 한다. CVD의 일환으로서 규제 기관의 의사소통 여부, 방법 및 시기와 관련하여 관할 구역별 차이가 있을 수 있다. 그러나 MDM은 문제가 평가된 후 적시에 고객 게시판, 통지 또는 기타 수단을 통해 정보를 개발하고 배치해야 한다. MDM은 적시의 의사소통에 관한 구체적인 관할 요구 사항을 알고 있어야 한다.

취약점이 아예 없는 소프트웨어 지원 의료기기란 없다. 따라서 CVD 참여는 일상적인 실무의 일부가 되어야 한다. MDM의 사이버보안 상태를 보여주는 지표의 역할을 하는 것은 취약점이 많고 적고가 아니라, 이에 대응하는 일관성과 적시성이다. 따라서 CVD는 환자의 건강과 안전을 개선하는 데 도움이 되기 때문에 의료기기 사이버보안에 대한 MDM의 사전 예방적 접근 방식의 일부가 되어야 한다. 사전 예방적 CVD와 관련하여 MDM은 다음을 수행해야 한다.

- 사이버보안 취약점 및 위험의 식별 및 감지를 위해 사이버보안 정보 출처를 모니터링한다.
- 조정된 취약점 공개 정책 및 실무를 채택한다(ISO/IEC 29147:2014:

정보 기술 - 보안 기법 - 취약점 공개(Information Technology - Security Techniques - Vulnerability Disclosure). 이러한 실무에는 기간 내에 취약점 발견자에게 초기 취약점 보고서를 수신했다는 사실을 알리는 과정이 포함된다.

- 취약점 유입 및 처리에 관한 절차를 수립하고 전달한다(ISO/IEC 30111:2013: 정보 기술 - 보안 기법 - 취약점 처리 절차(Information Technology - Security Techniques - Vulnerability Handling Processes). 이러한 절차는 취약점의 출처(예: 보안 연구원 또는 HCP 등)에 관계없이 명확하고 일관되며 재현할 수 있다.
- 확립된 보안(예: CVSS) 및 임상(예: ISO 14971:2019) 위험 평가 방법론에 따라 보고된 취약점을 평가한다.
- 가능한 경우, 개선책을 개발한다. 가능하지 않은 경우, 배치 실패를 보고하고 변경 사항을 원래대로 되돌리는 확립된 방법으로 적절한 취약점 완화 및/‘또는 보상적 통제를 개발한다.
- 필요시 규제 기관과 협력하여 곧 공개될 취약점 관련 정보를 확보한다.
- MDM의 현재 이해를 바탕으로 범위, 영향, 위험 평가를 포함한 취약점을 이해관계자에게 설명하고, 취약점 완화 및/또는 보상적 통제를 설명한다. 이해관계자도 상황 변화에 따라 최신 정보를 알고 있어야 한다.

MDM은 자체 고객에게 전달하는 것 외에도, 전 세계적으로 자사의 취약점을 공개할 수 있도록 조정하는 것이 좋다. 컴퓨터 비상 대응팀(CERT) 및 이와 동등한 조직은 CVD 절차 전반에 걸쳐 취약점 발견자 및 MDM과 협력하는 경우가 많다. 특히 CERT는 국제적인 및 지역

CERT 권고 사항을 현지 언어로 번역하여 공개하는 역할을 자주 담당한다. CVD에 관한 자세한 내용은 CERT® 조정된 취약점 공개에 대한 CERT 지침(Guide to Coordinated Vulnerability Disclosure)을 참조해야 한다.

6.3.2 규제 기관

규제 기관은 MDM과 취약점 발견자 간의 취약점 평가/평가, 영향 분석, 완화/개선 절차의 조정을 지원함으로써, 궁극적으로 대중에게 취약성 공격 위험을 완화하기 위해 필요한 관련 정보를 적시에 전달할 수 있게 된다. CVD가 모범 실무로 인식되기 때문에 이 의사소통에는 해당하는 경우 전 세계적이며 동시다발적인 의사소통이 포함된다.

6.3.3 취약점 발견자(보안 연구원 등 포함)

취약점이 발견되면 관련 MDM 또는 적절한 정부 개체와 같은 조정에 관여하는 서드파티에게 이를 직접 보고해야 한다. 그런 다음 MDM은 평가 및 개선 과정 동안 취약점 발견자와 함께 조정하고 소통해야 한다.

마지막으로, 취약점 발견자와 MDM은 취약점을 공개하는 사안을 조정해야 한다. 미국 국가통신정보국(NTIA: National Telecommunications and Information Administration) /미국 상무부, 취약점 공개 태도 및 조치: NTIA 인식 및 채택 그룹의 연구 보고서(2016년 12월)에서 채택한 바와 같이, 조정된 공개란 MDM이 발견자에게 응답하고 실제 상황에서 해당 취약점을 이용한 공격의 증거가 없는 한, 취약점 발견자는 수정 또는 기타 완화를 이용할 수 있을 때까지 해당 정보를 공개하지 않는

것을 의미한다. 발견자가 수정 전에 취약점을 공개한 경우, 발견자와 MDM은 최소한 가능한 모든 범위의 완화를 설명하여 HCP 및/또는 환자를 포함한 사용자가 기기를 안전하고 보안에도 안전한 상태에서 작동할 수 있는 가장 권한이 많은 위치에 자리 잡을 수 있도록 조정해야 한다.

6.4 취약점 개선

취약점 개선과 관련된 조치는 환자 피해의 위험을 줄이는 데 필수적이다. 개선에는 환자 통지를 포함한 다양한 범위의 작업이 포함될 수 있다. 이처럼, 이 절차에서는 여러 이해관계자 그룹이 중요한 역할을 수행하고 있으며, 해당 역할에 관하여 아래에 더 자세히 설명되어 있다.

6.4.1 MDM

a. 위험 관리

의료기기의 사이버보안 취약점에 대한 모든 대응의 첫 단계는 위험 평가이다. ISO 14971:2019에 약술된 위험 관리는 의료기기 분야에서 확실히 자리 잡은 확고한 실무이다. 이 실무는 취약점의 사이버보안 위험을 평가하고 위험 관리와 연관된 사이버보안 위험 관리 절차를 수립하여 MDM과 규제 기관이 환자의 안전에 미치는 영향을 판단하는 데 적용되어야 한다. 그다음에 환자 안전의 맥락에 근거한 개선 전략을 개발하고 합의할 수 있다. 이러한 접근 방식의 효과를 높이기 위해, 특히 인식된 위험 및 적절한 조치의 정당성과 관련된 정보를 규제 기관과 MDM 간에 공유해야 한다. 위험 평가 결과를 통해 개선 조치의 우선

순위와 시기를 파악할 수 있기 때문에, MDM과 규제 기관 각자의 위험 인식이 크게 다를 경우 적절한 개선 전략에 서로 합의하지 못할 가능성이 높다.

또한 MDM과 규제 기관은 위험 관리, 품질 관리, 규제에 익숙하지 않은 다른 이해관계자가 인식하는 위험을 고려해야 한다. 이에 따라 MDM이 보안 취약점에 대응하는 방법 및 설정한 대응 기간에 관한 기대치가 달라질 수 있다. 마찬가지로 일부 이해관계자는 취약한 기기를 충분히 보호하기 위해 배치된 환자 피해 위험을 허용할 수 있는 수준으로 완화할 수 있는 보상적 통제와 같은 위험 감소 메커니즘을 이해하지 못할 수 있다. 환자를 위험에 과도하게 노출시키는 부정확한 정보는 의료 기술에 대한 신뢰의 위기를 초래할 수 있다.

모든 이해관계자는 의료기기와 관련된 다른 위험과 마찬가지로 사이버 보안 취약점이 환자와 사용자에게 제기되는 위험에 비례하여 관리된다는 점을 인식해야 한다.

b. 서드파티 컴포넌트

서드파티 컴포넌트는 소프트웨어나 하드웨어와 같이 의료기기 공급망의 핵심 부분이다. 이러한 컴포넌트는 자체적으로 위험을 발생시킬 수 있고, MDM은 위험 관리, 품질 관리 및 설계 선택을 통해 해당 위험을 관리한다. MDM은 소프트웨어 및 하드웨어 컴포넌트의 사이버보안 영향을 관리해야 한다. 마찬가지로 컴포넌트와 관련된 시판 후 문제도 의료

기기의 보안에 영향을 미칠 수 있으며 MDM은 이러한 위험을 관리해야 한다. 사용자는 운영 체제 또는 프로세서와 같은 기본 컴포넌트의 보안 취약점이 의료기기에 어떤 영향을 미치는지 MDM이 이해하고 있으리라 기대한다.

서드파티 컴포넌트의 취약점에 대한 대응은 MDM이 자사 취약점에 대한 대응과 동일하게 이루어져야 한다. 즉, 지속적인 위험 관리 및 고객 및 사용자와의 정보 공유가 수행되어야 한다. MDM은 서드파티 취약점(예: 업데이트 가용성)에 대한 해결 일정을 통제할 권한이 없을 가능성이 높지만, 여전히 환자와 사용자에 대한 위험을 줄이기 위한 조치를 취해야 한다.

c. 의사소통

본 문서의 다른 장에서 논의한 바와 같이, 위험을 관리하기 위해서는 정보가 필요한 사람들과 명확하고 간결한 의사소통을 하는 것이 필수적이다. 또한, 위험 관리 인력에게 필요한 기술적 전문 지식수준이 어느 정도인지 인지해야 한다. 의사소통에는 취약점 해결을 위한 일정(예: 수정 사항이 제공되는 시기), 해결을 위한 메커니즘(예: 패치 배치 방법), CVSS 점수와 같은 취약점 점수, 취약점 공격 지수(예: 낮은 기술 수준) 및 방법(예: 원격) 및 임시 위험 완화 조치(예: 보다 영구적인 해결책을 기다림과 동시에 보상적 통제 사용 등의 취해야 할 조치)가 포함되어야 한다.

d. 개선 조치

이해관계자의 조치는 기기 유형, 규제 관할 구역, 사용자/환자 안전에

대한 위험, 의도된 목적을 포함한 여러 요소에 따라 달라진다. 그러므로 본 문서에서는 모든 기기에 예상되는 특정 조치를 자세히 설명하지 않는다. 그러나 모든 취약점 개선 조치의 기반이 되는 원칙은 다음과 같다.

- 현지 규제 요구사항 준수
- 안전성 및 필수 성능 원칙 준수
- 환자 및 사용자에 대한 위험을 줄이기 위해 이해관계자와 정보 공유
- 합의된 개선책을 달성하기 위한 이해관계자와의 협력
- 위험별 적시의 개선 조치

기기에 충분한 기본 또는 고유 보호 조치가 없고 업데이트가 가능하지 않은 경우, 보상적 통제로서 위험 완화 대안이 적용되어야 한다. 예를 들어, 기기와 의료 IT 네트워크 사이에 방화벽을 설치하거나 의료 IT 네트워크에서 기기를 제거하는 등의 대안이 있다. 일반적으로 이러한 보상적 통제는 MDM이 제공한 정보를 기반으로 HCP가 실행한다.

규제 기관은 관할 구역의 법률에 따라 운영되며, 이는 해당 시장의 의료기기에 개선 조치가 적용되기 전에 규제 기관에서 특정 사항을 요구할 수 있음을 의미한다. MDM은 취약점 개선 조치를 계획할 때 이 점을 고려해야 한다. 조기에 규제 기관에 통지하여 MDM의 개선 활동을 방해하거나 지연시키지 않도록 해야 한다. 조기에 규제 기관에 통지하면 규제 절차나 필요한 조치를 시작하는 동시에 개선책을 지원하고 이해관계자와 이들의 기대치(예: 사용자, 언론, 대중)를 관리할 수 있는 충분한

시간을 확보할 수 있다.

보안 취약점에 관한 정보는 전 세계 경제에 급속도로 빠르게 퍼지며 보안 취약점 공격으로 인한 파장은 몇 초 만에 전 세계에 도달할 수 있다. 따라서 취약점을 개선하기 위한 전 세계적으로 조정된 전략이 필요하다. 취약점이 한 관할 구역에서는 수정되고 공개되었지만 다른 관할 구역에서 해결되지 않은 채로 여전히 존재할 경우, 이는 적에게 우위를 넘겨주게 되어 환자뿐만 아니라 의료 부문 전체가 공격에 노출될 수 있다.

여러 시장에 공급하는 MDM의 경우, 정보 공개 및 개선 조치를 조정하여 시간 간극을 최소화해야 한다. MDM의 조정은 영향을 받는 제품이 유통되고 있는 곳의 모든 규제 기관과의 사전 예방적 의사소통으로 확대되어야 한다.

모든 이해관계자는 즉각적인 업데이트가 불가능하거나 바람직하지 않을 수 있고 임시 조치가 환자의 안전을 보장하는 데 있어 중요할 수 있다는 점을 인식해야 한다. 이는 이해관계자가 이러한 조치를 MDM이나 규제 기관의 직접적인 통제 밖에서 실행해야 하는 경우에 특히 중요하다. 예를 들어, 일부 조치의 경우 병원 IT 부서만 수행할 수 있다. 개선 전략 실행의 성공 여부는 효과적인 정보 공유 및 이해관계자 관리(사용자 및 언론 포함)에 따라 결정되는 경우가 많다. 개선 조치가 이상적이기는 하지만, 항상 가능한 것은 아니라는 점을 인식하고, 그러한 상황이 발생한 경우, 적절한 위험 완화 및 보상적 통제를 적용

해야 한다.

6.4.2 HCP 및 환자

a. 업데이트

환자는 전문 의료 시설과 가정 의료 환경에서 의료 서비스를 받으며, 각 사용 환경은 업데이트를 위한 고유한 고려 사항과 관련되어 있다.[2] 예를 들어, 가정 의료 환경에서 사용자는 환자, 간병인, 신뢰할 수 있는 이웃 또는 가족이 될 수 있다. 이 절에서는 업데이트에 대한 일반적인 지침을 제공하고 이어지는 절에서는 각 사용 환경에 해당하는 특정 고려 사항을 설명한다.

IEC 62304:2006+AMD1:2015의 6.2.5절, 의료기기 소프트웨어 - 소프트웨어 수명 주기 절차에 따라, MDM은 사용자와 규제 기관에 출시된 의료 소프트웨어의 문제와 변경 사항의 획득 및 설치 방법에 관한 정보를 알려야 한다. MDM이 식별하고 현지 규제 당국이 승인한 의료기기의 특정 사용자는 관련 설치 지침에 따라 MDM이 제공하는 업데이트를 실행해야 한다. 이러한 사용자는 MDM의 지침에 따라 웹페이지에 일반적으로 제공되는 서비스 게시판 및 기타 정보에 접근해야 한다.

합리적인 일정 내에 업데이트를 적용할 수 없는 경우, MDM은 보상 통제(예: 의료 IT 네트워크 분할) 또는 사용자가 프로그래밍할 수 있는

2) IEC 60601-1-11:2015, 전기의료장비- 1~11부: 기본 안전 및 필수 성능을 위한 일반 요구 사항 - 보조 표준: 가정 의료 환경에서 사용되는 의료 전기 장비 및 의료 전기 시스템에 대한 요구 사항에서는 '가정 의료 환경'을 '전문 의료 시설 환경을 제외한 환자의 거주지 또는 환자가 있는 기타 장소'로 정의하고, 예로는 '자동차, 버스, 기차, 보트, 비행기, 휠체어 또는 실외 산책' 등을 제시한다.

의료기기의 설정 변경을 권장할 수 있다. 특정 유형의 취약점으로 인한 환자 피해 위험을 줄이기 위해 현지 규제 당국은 MDM이 의료기기, 부속품 또는 지원 생태계(예: 소프트웨어 업데이트 서버)의 특정 기능을 비활성화하도록 지시할 수 있다. 두 경우 모두, 사용자는 MDM의 지침을 따라야 하고 해당하는 경우 사용 환경과 관련된 위험을 평가해야 한다.[3]

표 2는 공동 보안 계획에 문서화된 패치 방법을 간략히 정리한 것이다.[4] 표의 맨 오른쪽 열은 MDM 승인 업데이트를 실행하는 식별된 사용자의 기본 책임을 설명한다.

표 2: 업데이트 방법 및 실행에 대한 사용자 책임

업데이트 방법	요약 설명	사용자 책임
원격 업데이트	업데이트는 MDM이 제공하는 보안에 안전한 승인 원격 서비스 및 지원 플랫폼을 통해 적용된다.	MDM이 제공하는 지침에 따라 원격 연결을 확인해야 한다.
사용자 관리	승인된 업데이트는 제품 또는 컴포넌트를 제공하는 서드파티로부터의 직접 다운로드를 포함하여 지정된 출처에서 고객이 검색하고 설치할 수 있도록 제공된다.	MDM이 제공하는 지침에 따라 업데이트를 검색하고 설치해야 한다.
서비스 방문	현지 서비스 시설이 사이버보안 업데이트(현장 서비스 포함)를 관리한다. 참고로, 이 방법은 잘못된 업데이트로 인해 심각한 피해가 발생할 것으로 예상되어 해결을 위해 현지 서비스 직원이 필요할 수 있는 경우에 적용된다.	의료기기를 서비스 시설에 제공하거나 현장 서비스 방문을 지원하거나 전문 의료 시설로 이동해야 한다.

3) 사용자가 특정 상황에서는 위험을 적절하게 평가할 수 없다는 점을 인정한다

4) 의료기기 및 보건 IT 공동 보안 계획, 미국 의료 및 공중 보건 부문 조정 위원회(HSCC), 2019년 1월. 첫 두 열에는 명확성을 개선하기 위한 사소한 변경 사항이 포함되어 있으며 '임시' 패치 방법은 제거되었다(유효성이 확인된 패치만 고려함).

참고로, 서비스 방문의 경우, 사용자는 업데이트 설치를 위해 자격을 갖춘 전문가와 상호 작용할 책임이 있다.

b. 의료 시설 환경에 대한 고려 사항

의료 시설에서 환자는 현지 규제 요구 사항에 따라 면허가 있거나 면허가 없어도 자격을 갖춘 의료 전문가(예: 간호사, 의사)에 의해 진료를 받게 된다. 환자는 안전하고 효과적인 의료기기 작동을 보장하기 위해 보안 관련 지침을 포함하여 HCP가 제공하는 지침을 따라야 한다.

IEC 80001-1:2010 의료기기 통합 IT 네트워크에 대한 위험 관리 적용 - 1부: 역할, 책임, 활동(Application of risk management for IT Networks incorporating medical devices — Part 1: Roles, responsibilities and activities)의 3.2절에서는 의료 IT 네트워크에 배치된 의료기기의 유지 관리를 포함하여 '책임 조직'의 위험 관리 책임을 설명한다. 책임 조직은 환자의 직속 HCP와 다를 수 있다. 업데이트는 위험 통제 조치의 한 유형이며 4.4.4.3 절에서는 다음과 같이 구체적인 지침을 제공한다.

"이 의료기기 내의 위험 통제 조치는 MDM 또는 책임 조직이 사용 지침 또는 MDM의 문서화된 승인 절차에 따라서 실행해야 한다. … MDM의 문서화된 동의 없이 책임 조직이 수행하는 의료기기에 대한 변경은 권장하지 않는다."

이러한 권장 사항은 의료 IT 네트워크의 효율적이고 안전한 관리를

보장하기 위해 개발되었다. 일반인은 의료 IT 네트워크에 연결된 의료 기기의 업데이트를 설치할 수 없어야 한다.

IEC 80001-1에서 강조한 바와 같이, 책임 계약은 의료 IT 네트워크의 기기 관리는 모든 당사자의 공동 책임임을 이해한다는 사실을 확실하게 할 수 있는 한 가지 선택 사항이다. MDM이 의료기기의 특정 기능을 비활성화하라는 지시를 받은 경우, HCP는 임상 워크플로우를 평가하여 환자 안전이 유지되도록 해야 한다.

c. 가정 의료 환경에 대한 고려 사항

가정 의료 환경에 해당하는 대상으로 FDA의 관련 지침인 가정용 기기의 설계 고려 사항(Design Considerations for Devices Intended for Home Use)에 명시된 바와 같이 다양한 잠재적 사용자가 있다.

"가정용 기기의 사용자는 일반적으로 전문 의료 시설에서 의료기기를 작동하는 의료 전문가와 다르다. 가정용 기기 사용자의 경우, 다양한 범위의 신체적, 감각적, 인지적 능력과 장애를 갖고 있을 수 있으며, 가정용 기기 설계에서 고려해야 할 정서적 차이가 있을 수 있다."

가정 의료 환경을 위한 업데이트 방법의 적용 가능성이란 의료기기 위험 분류, 자원 요구 사항(예: 고속 인터넷 연결) 및 사용성을 포함한 많은 요인의 기능을 의미한다. 다양한 범위의 사용자 기능으로 인해 많은 가정용 기기의 경우 표 1에 나열된 '서비스 방문' 업데이트

방법이 필요하다. 이식형 의료기기를 업데이트하는 경우, 환자의 HCP와 직접 상호 작용해야 할 수 있다.

일부 가정용 기기, 특히 소프트웨어 의료기기(SaMD)로 분류된 기기는 원격 업데이트 또는 사용자가 관리하는 패치 방법을 수용한다. 원격 업데이트의 경우, 최소한의 사용자 상호 작용만 필요하지만, HCP가 수립한 절차에 따라 환자의 동의가 필요한 경우가 많다. 두 업데이트 방법 중 어느 것이든, 환자는 HCP와 해당하는 경우 MDM이 제공하는 지침을 따라야 한다.

환자가 해외로 이동하고자 하는 경우, HCP 또는 MDM에 문의하여 기기의 소프트웨어 유지 관리 옵션을 이해해야 한다.

6.4.3 규제 기관

시판 후 업데이트

위협 행위자는 취약점 공격 기법을 지속해서 조정하고 발전시키고 있다. 그 결과, 기기의 사이버보안 복원력(‘사이버 위생’)을 향상하거나 취약점을 개선하거나 개선할 수 없는 취약점의 위험을 완화하기 위해 빈번한 소프트웨어 유지 관리 활동이 필요하다. ‘오직 사이버보안을 강화하기 위해’ 진행한 각 변경 사항마다 최고 수준의 규제 검토를 받게 된다면, 그로 인해 과중 된 검토 부담은 곧 규제 당국 대부분의 과부하로 이어질 것이다.

규제 당국은 사이버보안의 맥락에서 소프트웨어 변경으로 인한 출시 전 승인 필요 여부를 판단하기 위해 다음 두 가지 기본적인 질문을 설정해야 한다.

1. 해당 변경이 오직 사이버보안을 강화하기 위한 것이고 소프트웨어나 기기에 다른 영향을 미치지 않는다고 결정되었는가?

MDM은 필요한 분석, 검증 및/또는 유효성 검사를 수행하여 이러한 변경이 기기의 안전성 또는 성능에 영향을 미치지 않는다는 점을 확인할 수 있도록 시스템을 평가해야 한다. MDM은 소프트웨어 또는 기기의 다른 측면에 관한 변경의 부수적 또는 의도치 않은 영향을 인지한 경우, 규제 당국은 제안된 수정, 사전 배치에 대한 검토가 적절하다고 결정할 수 있다.

2. 해당 변경이 환자 피해와 관련된 허용할 수 없는 잔존 위험과 관련된 취약점의 위험을 개선하거나 줄이기 위해 시행되었는가?

시판 후 취약점 위험 평가는 취약점 공격 가능성 및 잠재적인 환자 피해의 심각성에 대한 평가에 기반해야 하며, 잔존 위험의 허용 가능성 유무를 결정하는 데 사용된다. 참고로, ‘환자 피해’의 정의는 ISO 14971:2019, 의료기기 - 의료기기에 대한 위험 관리의 적용(Medical devices — Application of risk management to medical devices)에 정의된 ‘피해’의 하위 집합이다.[5] 환자 피해에 대한 좁은 의미의 정의는

5) ISO 14971:2019에서는 ‘피해’를 ‘인간의 건강에 대한 신체적 부상 또는 손상, 재산 또는 환경에 대한

공중 보건을 보호하기 위해 필요한 변경 사항에 대한 규제 검토의 우선 순위를 정하는 데 기본적으로 영향을 미친다.

표 3은 다양한 유형의 소프트웨어 유지 관리 활동에 필요한 규제 감독을 고려할 때 규제 기관이 고려해야 할 권장 프레임워크를 제시하고 있다. 이 표에 제시된 수준은 규정 요구 사항이 아니지만, 권장 수준의 규제 감독 지침을 제공한다.

표 3: 소프트웨어 업데이트 및 권장 수준의 규제 감독

업데이트 목적		제안된 규제 요구사항수준	예시
보안 향상('사이버 위생')		하	소프트웨어 의료기기(SaMD) 애플리케이션('앱') 제조업체에 심층 방어 전략을 지원하기 위해 보안 통제를 추가하는 호스트 운영 체제 업데이트 정보가 제공된다. SaMD 앱의 경우, 호스트 운영 체제의 낮은 수준의 인터페이스 변경 사항과 호환되도록 수정이 필요하다. 관련된 SaMD 앱 수정 사항은 알려진 취약점과 전혀 관련이 없다.
개선할 수 없는 취약점에 대한 취약점 개선 또는 위험 감소 전략	허용할 수 있는 환자 피해의 잔존 위험성	중	MDM은 혈액가스 분석기가 멀웨어에 감염되었고 이에 따라 기기의 데이터가 변경될 수 있다는 우려의 사용자 불만을 접수한다. MDM 조사 및 영향 평가 결과는 멀웨어의 존재를 확인하고 멀웨어가 기기를 통해 저장되거나 입력되는 암호화되지 않은 데이터를 조작하지 않음을 확인한다. 멀웨어가 기기의 안전성 및 필수 성능에 영향을 주지 않으며, MDM의 위험 평가에서 해당 취약점으로 인한 환자 피해 위험이 허용할 수 있는 수준인 것으로 판단한다.[6]
	허용할 수 없는 환자	상	MDM은 개방된 미사용 통신 포트를 알고 있다. MDM은 취약점 발견자에게 취약점 보고서를

손상'으로 정의하는 반면, '환자 피해'는 이 정의의 첫 번째 구에만 해당한다.

	피해의 잔존 위험성		수신했음을 알리고, 이후 분석에서 기기의 설계 기능이 기기의 안전성 및 필수 성능을 손상하는 데 사용될 수 있는 무단 펌웨어를 기기로 다운로드하는 위협을 막지 못한다고 판단한다. 해당 취약점과 관련된 심각한 부작용이나 사망은 보고되지 않았지만, 위험 평가는 환자 피해의 위험을 허용할 수 없는 수준이라고 결론을 내린다.[7]

제안된 소프트웨어 변경이 여러 취약점에 영향을 미치거나 아니면 대안적으로 '사이버 위생'을 향상시키고 최소한 하나의 취약점에 영향을 미치는 경우, MDM은 후속 조치를 알리기 위해 표 3에 나와 있는 적용 가능한 최고 수준을 고려해야 한다. 예를 들어, 단일 소프트웨어 변경이 시스템 보안을 강화하고 취약점 A의 위험(허용 가능한 환자 피해의 잔존 위험)을 줄이며 취약점 B(허용 불가능한 환자 피해의 잔존 위험)를 개선할 수 있다. 이 경우, 취약점 B와 관련된 '상' 수준의 규제 요구 사항이 적용된다.

모든 수준에 대해서, 규제 당국은 MDM은 확립된 수명 주기 절차와 IEC 62304:2006/AMD 1:2015에서 명시된 사항을 포함한 소프트웨어 유지 관리를 위한 기타 규제 요구 사항을 준수하고 있다는 증거를 재량에 따라 요청할 수 있다.

6) 업계 및 식품의약국(FDA) 실무자용 지침, 의료기기의 사이버보안에 대한 시판 후 관리(Guidance for Industry and Food and Drug Administration Staff, Postmarket Management of Cybersecurity in Medical Devices)에서 제공한 예시이다. 2016년 12월

7) Ibid.

6.5 사고 대응

6.5.1 MDM

MDM은 환자를 포함한 제품과 고객에게 영향을 미칠 수 있는 사이버 보안 사고 및 사건에 대비해야 한다. 그러므로 MDM은 확장 가능한 사고 대응 관리 정책을 수립하고 제품 포트폴리오에 기반하여 사고 대응 팀을 구축해야 한다. 사고 대응 팀의 목적은 사이버보안 사고를 평가하고 이에 대응하면서 배운 결과를 활용해 다음 사고 발생 시 적시에 적절한 조치를 취할 수 있도록 필요한 조정, 관리, 피드백, 의사소통을 제공하는 적절한 역량을 키우는 데 있다.

준비에는 사고 관리 정책 수립, 세부 사고 대응 계획 개발, 사고 대응 팀 구축, 일상적으로 진행하는 사고 대응 테스트 및 연습, 그리고 배운 교훈을 통해 이러한 역량을 지속적으로 향상시키는 작업이 포함된다.

ISO/IEC 27035에 정의된 사고 관리에는 개괄적으로(더 자세한 내용은 역할 및 책임 절 참조) 계획 및 대비, 감지 및 보고, 평가 및 결정, 대응 및 교훈이 포함된다(항목별 설명은 부록 A 참조).

a. 역할 및 책임

사고 대응 팀은 관리자, 계획, 모니터링, 대응, 실행, 분석, 때로는 외부 전문가로 나눌 수 있다. 각 그룹마다 서로 다른 역할과 책임이 있다. 팀에서는 기술과 지식을 바탕으로 이러한 그룹에 구성원을 배정해야 하며,

일부 자리의 경우, 두 명 이상의 팀 구성원이 채울 수 있다. 관련 그룹에 배정된 구성원은 동일하거나 유사한 업무를 담당해야 한다. 이러한 그룹 역할에 관한 자세한 내용은 부록 A에서 확인할 수 있다.

b. 의사소통 요구 사항

사이버보안 사고 및 사건을 보고하기 위해 MDM의 연락처 정보를 고객에게 제공하거나, 아니면 정기 고객 지원 채널을 통해 제출해야 한다. 사고 대응 팀은 사고의 영향을 받는 모든 이해관계자에게 업데이트를 제공하기 위한 일상적인 업무 방식을 수립하고, 최초 발견 후 가능한 한 빨리 고객에게 관련 정보를 전달할 수 있도록 노력해야 한다 (MDM은 적시의 정보 전달과 관련된 구체적인 관할 요구 사항을 숙지해야 한다). 사고가 발생했을 경우, MDM이 적시에 게시판 공지나 통지를 할 수 있을지는 고객과의 시기 적절하고 정확한 의사소통에 달려 있다.

환자 안전과 개인정보 보호에 영향을 미치는 의료기기 사이버보안 사고는 규정에 따라 해당 규제 기관에 보고해야 한다. 수사 과정을 통해 범죄 행위가 확인된 경우, 현지 및 해당 법 집행 기관에 통지해야 한다. 국제적인 사이버보안 공격 및 사건의 추가 조정을 위해 CERT와 ISAO에 연락해야 한다.

6.5.2 HCP

HCP는 보안 사고를 완화 또는 해결하고 내부 및 외부 이해관계자에게 관련 정보를 공개하기 위한 메커니즘과 보안 사고를 처리하기 위해

필요한 정책을 수립해야 한다. 이를 위해서 HCP는 기기 취약점 완화를 위한 계획 및 자원 관리를 고려해야 한다. 여기에는 사고 발생 시 필요한 경우 예비 또는 추가 기기를 사용할 수 있도록 준비하는 것도 포함될 수 있다.

a. 정책 및 역할

HCP 조직에서 취약성 또는 보안 사고 처리 정책 및 역할을 시행해야 한다. 이러한 정책은 HCP가 MDM 공개 문서(예: 의료기기 보안을 위한 제조업체 공개 진술서(MDS^2), SBOM, 취약성/업데이트 정보), 정보 공유 기관 또는 참여 ISAO로부터 정보를 수신하고 전파하는 방법을 수립해야 한다. 이를 위해 정보 공유를 위한 연락처 목록을 정기적으로 유지 관리하고 검증해야 한다. 마찬가지로, 설치 전에 수립되고 정기적으로 검토되는 서비스 수준 계약(SLA)을 통해 MDM 및 기타 공급업체가 사고 발생 시 또는 사고 발생에 대한 대응으로 이행해야 하는 내용과 조건을 제공할 수 있다. HCP는 자체 보안 사고 대응 팀을 구축하는 것이 좋다.

b. 역할별 교육

각 관련 역할의 교육 요구 사항을 수립하고 정기적으로 검토하여 업데이트 필요 여부를 결정해야 한다. 보안 사고의 증거를 평가하는 보안 전문가는 실무 경험 외에도 보안 분석 교육을 받아야 한다. 사고 대응 과정에 참여하는 사람들은 실무 경험 외에도 해당 과정과 사고 대응 이론에 관한 교육을 받아야 한다. 교육 절차를 주기적으로 평가해야

하며, 해당 평가를 수행하기 위해 사고 대응 연습을 수행할 수 있다.

c. 분석 및 대응

HCP는 사고 또는 보고된 취약성의 영향을 평가하고 조사의 결과를 설명하는 정보를 제공하여 MDM을 포함한 이해관계자와 협력해야 한다. 해결을 위해 조치가 필요한 경우, 조사 현황 및 일정표를 결과에 포함해야 한다. HCP는 모범 실무 및 완화 조치를 포함한 안전 관련 정보를 환자에게 계속 제공해야 한다. 해결책에 개선 조치가 포함된 경우, 전체 시설에 개선 조치를 적용하기 전에 회귀 테스트를 포함한 유효성 검증을 수행해야 한다. 이러한 테스트를 통해 개선 조치가 기존 시스템 기능을 방해하지 않는다는 사실을 확인해야 한다. HCP는 필요한 경우 개선 및 완화 정보를 업데이트해야 한다.

6.5.3 의료기기 규제 기관

규제 기관도 의료기기 사이버보안 사고 대응에 참여해야 한다. 위의 MDM 대응 절에서 언급한 바와 같이, 규제 기관에 사이버보안 사고를 알려서 규제 기관에서 이를 인지하여 규제 의사 결정을 위한 추가 정보를 요청할 수 있고 필요한 경우 추가 조치를 취할 수 있도록 해야 한다. 해당하는 경우, 추가 조치에는 환자 안전 영향 평가, MDM이 제안한 편익/위험 평가, 이해관계자(사이버보안 연구원과 같은 비전통적 이해관계자 포함)와의 의사소통, 다른 정부 기관 및 규제 기관과의 참여가 포함될 수 있지만 이에 국한되지는 않다.

6.6 레거시 의료기기

본 IMDRF 지침의 목적을 위해, 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 없는(업데이트 및/또는 보상적 통제를 통해) 의료기기는 레거시 기기로 간주한다. 현재 사용 중인 많은 기기와 관련하여 초기 장치 설계 및 유지 관리 시 기기의 사이버보안을 고려하지 않았을 수 있기 때문에 레거시 조건은 전 세계 의료 생태계의 현황에서 특히 복잡한 문제를 제기한다. 의료기기 내 디지털 기술로의 전환으로 인해 구형 아날로그 기기에서는 결코 실현될 수 없는 확장된 기능이 제공됨에 따라 기기의 임상 유틸리티가 보안 지원 능력을 넘어서는 경우가 많아지면서 오늘날 문제가 더욱 악화되고 있다. 이러한 기술을 바탕으로 소프트웨어, 하드웨어, 네트워크 연결의 조합은 기기 수명에 대한 새로운 요구를 창출하고 있다. 기기 수명은 자본 장비(예: 스캐너 하드웨어)와 물품 컴포넌트(예: 서버, 워크스테이션, 데이터베이스, 운영 체제)로 구성되는 경우가 많다. 그러나 기기 연령이 레거시 상태의 유일한 결정 요인은 아니라는 점을 유념해야 한다. 즉, 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 없는 기기의 연령이 5년 미만일 수 있다. 이 기기의 경우, 연식과 상관없이 여전히 레거시로 간주한다. 반면에 15년이나 된 기기이더라도, 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 있는 기능을 유지하고 있다면 해당 기기는 레거시로 간주되지 않는다.

초기 기기 설계 및 개발 단계부터 시작되는 TPLC 의료기기 사이버보안 문제를 해결하기 위한 노력이 계속 발전하면서, 사용 기간 동안

사이버보안 위협으로부터 지킬 수 있는 합리적인 보호 기능을 유지하는 기기의 가용성이 점점 더 표준이 될 것이고, 현재 임상적으로 사용 중인 수많은 레거시 기기와 관련하여 관찰되는 이러한 불균형(HCP와 네트워크에 보안 위협을 가하는)이 줄어들 것이다. 본 IMDRF 지침의 다음 하위 절에서는 HCP에게 적절하게 사전 통지하여 비즈니스 연속성 계획을 수립할 수 있게 하면서, 레거시 기기(현재 사이버보안 위협으로부터 합리적으로 보호할 수 없는 기기)가 폐기/단계적으로 사용 중단되는 향후 최적의 의료기기 사이버보안 상태를 추진하는 개념 프레임워크를 명확히 설명한다(그림 2 참조).

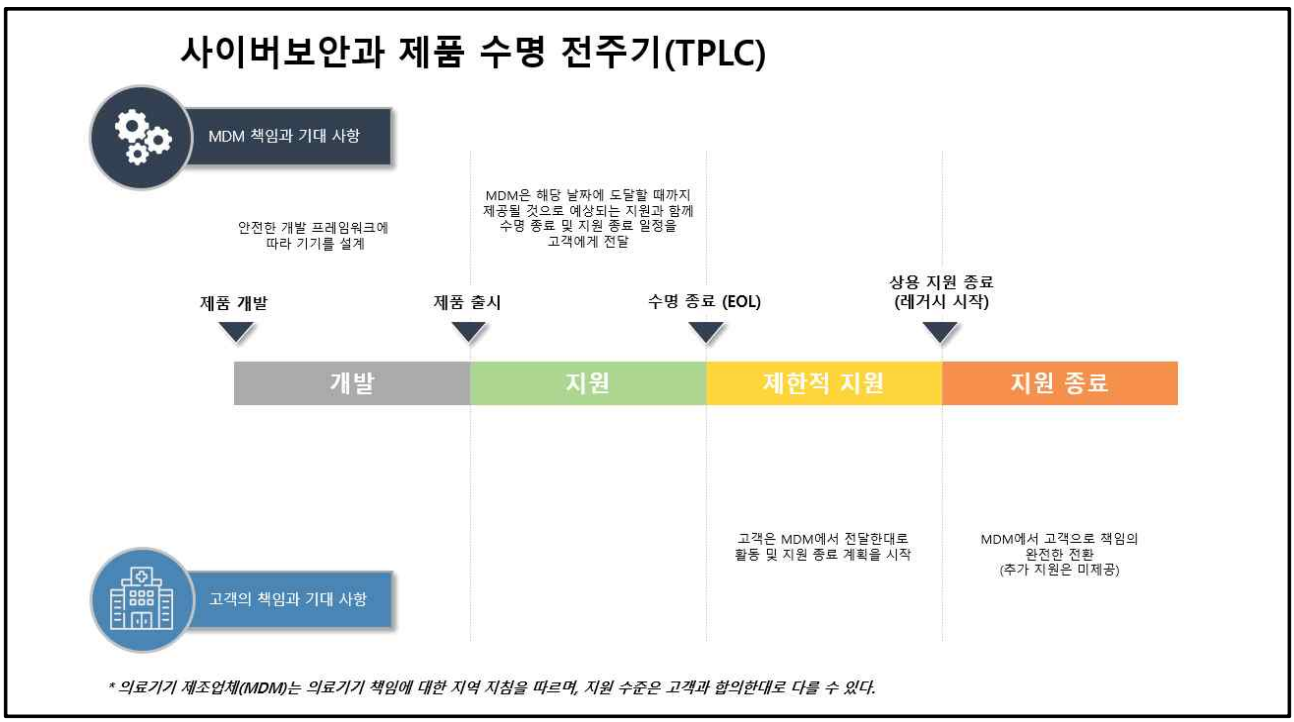

그림 2: 사이버보안을 위한 TPLC 기능으로서의 레거시 의료기기 개념 프레임워크

6.6.1 MDM

의료기기 사이버보안에 대한 관심은 그림 2에 나와 있듯이 상용 출시

훨씬 전에 기기 설계 및 개발 중에 시작된다. 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 있는 의료기기를 위한 전폭적 지원은 TPLC 프레임워크에 맞춰 MDM이 발행한 사이버보안 수명 종료(EOL)까지 지속적으로 이루어져야 한다. MDM의 사이버보안 EOL 날짜는 의료기기의 포괄적 사이버보안 지원을 제공할 수 있는 용량이 줄어들었음을 나타낸다. 사이버보안 EOL에 가까워지면 MDM은 기기의 사이버보안 지원 종료(EOS) 날짜를 명확하게 전달하는 동시에 고객에게 EOL 이후에 제공되는 제한적인 지원 소식을 알리는 통지를 전달해야 한다. 지정된 사이버보안 EOS 날짜가 지난 의료기기에 대해서는 지원이 이루어지지 않는다.

이 개념 프레임워크에 따라 의료기기가 사이버보안 EOS 날짜에 도달하는 경우, 이를 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 없는 레거시 의료기기로 간주해서 폐기해야 한다. EOS 날짜 이후의 기기 보안 및 지속적인 사용에 따른 위험 부담에 대한 책임은 해당 시점에서 HCP와 같은 고객에게 이전된다.

주목해야 할 점은 일부 기기의 설계 변경(예: 더 이상 지원되지 않고 보안 목적으로 패치할 수 없는 구식 운영 체제)이 실현 가능하지 않더라도 보상적 통제를 통해 일정 수준의 보호 기능을 제공할 수 있다는 사실이다. 사용 가능하고 성공적으로 배치된 보상적 통제가 존재하는 경우, 해당 의료기기를 해당 프레임워크에 따른 레거시로 간주하지 않는다. 필요한 경우, 규제 기관은 MDM이 보상적 통제를 활용하여

EOL 날짜 이후 현재의 기기 보안 문제를 해결하도록 권장할 수 있다. 이를 통해 HCP는 MDM이 더 이상 보안 지원을 제공하지 않을 때 EOS에 대한 비즈니스 연속성 계획을 수행할 수 있는 충분한 시간을 확보할 수 있다. 기기 설계, 취약성 관리, 고객과의 의사소통은 기기 사이버보안 문제를 해결하는 데 중요한 역할을 한다. TPLC 단계에 따른 MDM을 위한 권장 사항은 다음과 같다.

- 개발:
  a. 의료기기를 구성하는 하드웨어 및 소프트웨어 컴포넌트의 지원 수명 주기를 고려해야 한다.. 의료기기에 대한 포괄적인 지원을 제공하기 위해, MDM은 품질, 성능 및 보안 문제를 해결하는 소프트웨어/펌웨어 업데이트를 통해 해당 하드웨어 및 소프트웨어 공급업체의 지원을 받을 수 있어야 한다. MDM은 제품 사용 전반에 걸쳐 제품의 안전성과 효능을 지원해야 할 경우에 대비해야 한다. MDM은 HCP의 예상 기기 사용 수명 전에 컴포넌트에 대한 서드파티 공급업체의 지원이 종료될 수 있고, 이는 기기의 안전한 작동을 지원하는 MDM의 능력에 부정적인 영향을 미칠 수 있음을 고려해야 한다.
  b. 시큐어 개발 프레임워크에 따라 기기를 설계 및 개발하여 향후 레거시 기기의 수를 최소화해야 한다. 이러한 기기는 최소한 보안 기준을 충족해야 하고 업데이트 및 패치를 위한 메커니즘을 포함해야 한다.

- 지원:
  a. 위험 관리의 일환으로 기기의 TPLC에 맞춰, 의료기기에 허용할 수 없는 위험이 있는 취약점이 있는지 모니터링하고 최선의 대응을 제공하며 지속적인 위험 문서를 유지 및 보관해야 한다.
  b. 구매 및 설치 절차의 일부로 기기의 사이버보안 EOL 날짜를 포함한 주요 수명 주기 이정표를 명확하게 전달해야 한다. 이 시점에서 전달하는 내용에는 고객의 책임도 포함되어야 한다.
  c. 기기 컴포넌트에 대한 서드파티 공급업체의 지원 종료를 사전에 미리 고객에게 알려야한다.
  d. 사이버보안 EOS 날짜에 가까워졌을 때 고객에게 지속적이지만 제한적인 지원이 제공되고 EOS 날짜 이후에는 해당 기기가 지원되지 않는 레거시 상태로 간주된다는 점을 알려야한다. 이러한 정보를 고객에게 전달하는 과정은 EOL 날짜가 다가옴에 따라 이루어져야 하며, 이를 통해 HCP에 대한 기기 폐기/단계적 사용 중단 및 비즈니스 연속성 계획에 대한 사전 통지가 가능해질 것이다. 관련 정보를 명확하게 전달하면, 의료 기관은 기기의 위험뿐만 아니라 자신의 책임도 이해하게 되어 그에 따라 기기 폐기와 교체 계획, 예산을 수립할 수 있다.

- 제한적 지원(EOL이 이 지점부터 시작됨):
  a. 고객이 EOS 및 관련 고객 책임을 준비할 수 있는 충분한 시간을 확보할 수 있도록 사이버보안 EOS 날짜의 일정을 계속 전달해야 한다.
  b. 위의 지원 수명 주기 단계의 조치 ‘a’와 ‘c’를 계속해야 한다.

- 지원 종료(EOS: 이 지점에서부터 레거시로 간주됨):
  a. MDM으로부터 고객에게 책임을 완전히 이전한다. 기기에 대한 공식 사이버보안 EOS에 따라, 기기의 사용자는 어떠한 수준의 지원도 기대해서는 안된다.

6.6.2 HCP

HCP 상당수가 MDM이 발행한 사이버보안 EOL에서 제공한 기기의 수명보다 훨씬 더 긴 시간 동안 기기를 사용할 계획을 세운다. 그러나 시간이 지남에 따라 위협 환경이 변화하고 새로운 위협 상황이 등장함에 따라 구식 기술을 사용하는 데 따른 위험과 비용이 증가하고 있다. 이에 대해 MDM과 HCP가 서로 공동으로 책임을 져야 한다. 기기 수명 주기 단계에 따른 다음과 같은 권장 사항은 정의된 사이버보안 EOS 날짜를 미리 계획하기 위해 의료 HCP가 의료기기 관련 문제를 해결하는 데 도움이 될 것이다.

- 지원:
  a. TPLC 계획, 이해 및 투명성을 보장하기 위해 MDM의 명확한 연락처 및 정보 전달 절차를 요청해야 한다.
  b. 지원 수명 주기가 가장 짧은 소프트웨어 컴포넌트는 궁극적으로 이러한 기기의 지원 가능성과 보안에 영향을 미치게 되므로 SBOM을 요청해야 한다. SBOM을 획득하면 고객은 기기 수명 주기에 영향을 미치는 컴포넌트를 보다 잘 이해할 수 있고, 보상적 통제와 같은 위험 통제 조치를 위한 추가 하드웨어에 관한 정보를 포함

할 수 있다.

c. MDM, 서드파티 서비스 대리인 또는 내부 자원 및 통제를 통해 사용 중인 의료기기를 적절히 지원하고 유지 관리해야 한다. 여기에는 네트워크 보안, 자산 보안, ID 및 접근 관리, 보안 작업에 대한 적절한 지원이 포함된다.

d. 환경 내에서 진화하는 새로운 위험을 평가하고 네트워크 세분화, 사용자 접근 역할, 위험 평가, 보안 테스트, 네트워크 모니터링 등을 포함하되 이에 국한되지 않는 적절한 완화를 통해 위험을 통제하기 위해 모든 노력을 기울여야 한다.

e. MDM의 사이버보안 EOS 날짜를 미리 계획하여 지원되지 않는 레거시 기기(환자의 안전 및 의료 네트워크 보안을 위협할 가능성이 있음)를 적절하게 단계적으로 사용 중지하고 보안에 안전하고 지원 가능한 의료기기로 교체해야 한다.

- 제한적 지원:

  a. 위의 지원 수명 주기 단계의 조치 'c', 'd', 'e'를 계속해야 한다.

- 지원 종료(EOS):

  a. 기기를 폐기할 때 치료의 연속성에 영향을 미칠 수 밖에 없는 경우, 사이버보안 EOS 날짜 이후 지속적인 사용에 대한 보안 위험 부담 및 기기 보안 관리에 대한 책임을 진다.

7.0 참고 문헌

7.1 IMDRF 문서

1. 소프트웨어 의료기기 위험 분류 및 해당 고려 사항을 위한 잠재적 프레임워크 IMDRF/SaMD WG/N12:2014(2014년 9월)
2. 의료기기 및 IVD 의료기기의 안전성 및 성능 기본 원칙 IMDRF/GRRP WG/N47 FINAL:2018(2018년 11월)

7.2 표준안

3. AAMI TIR57:2016 의료기기 보안 원칙 - 위험 관리

4. AAMI TIR 97:2019, 의료기기 보안 원칙 - 기기 제조업체의 시판 후 위험 관리

5. IEC 60601-1:2005+AMD1:2012, 전기의료장비 - 1부: 기본 안전 및 필수 성능에 대한 일반 요구 사항

6. IEC 62304:2006/AMD 1:2015, 의료기기 소프트웨어 - 소프트웨어 수명 주기 절차

7. IEC 62366-1:2015, 의료기기 - 1부: 의료기기에 대한 사용성 엔지니어링 적용

8. IEC 80001-1:2010, 의료기기를 통합한 IT 네트워크에 대한 위험 관리 적용 - 1부: 역할, 책임, 활동

9. IEC TR 80001-2-2:2012, 의료기기를 통합한 IT 네트워크에 대한 위험 관리 적용 - 2-2부: 의료기기 보안 요구, 위험 및 통제의 공개 및 의사소통을 위한 지침

10. IEC TR 80001-2-8:2016, 의료기기를 통합한 IT 네트워크에 대한 위험 관리 적용 - 2-8부: 적용 지침 - IEC 80001-2-2에 규정된 보안 역량 확립 표준 지침

11. ISO 13485:2016, 의료기기 - 품질 관리 시스템 - 규제 목적을 위한 요구 사항

12. ISO 14971:2019, 의료기기에 대한 위험 관리 적용

13. ISO/TR 80001-2-7:2015, 의료기기 통합 IT 네트워크에 대한 위험 관리 적용 - 적용 지침 - 2-7부: 의료 제공 조직(HDO)의 IEC 80001-1 준수 자체 평가 방법에 대한 지침

14. ISO/IEC 27000 집합 - 정보 보안 관리 시스템

15. ISO/IEC 27035-1:2016, 정보 기술 - 보안 기법 - 정보 보안 사고 관리

- 1부: 사고 관리 원칙

16. ISO/IEC 27035-2:2016, 정보 기술 - 보안 기법 - 정보 보안 사고 관리 - 2부: 사고 대응을 위한 계획 및 대비 지침

17. ISO/IEC 29147:2018, 정보 기술 - 보안 기법 - 취약점 공개

18. ISO/IEC 30111:2013, 정보 기술 - 보안 기법 - 취약점 처리 절차

19. ISO/TR 24971:2020, 의료기기 - ISO 14971의 적용 지침

20. UL 2900-1:2017, 네트워크 연결 가능 제품의 소프트웨어 사이버보안 표준, 1부: 일반 요구 사항

21. UL 2900-2-1:2017, 네트워크 연결 가능 제품의 소프트웨어 사이버 보안, 2-1부: 의료 및 복지 시스템의 네트워크 연결 가능 컴포넌트에 대한 특정 요구 사항

7.3 규제 지침

22. ANSM(초안): 수명 주기 동안 소프트웨어를 통합하는 의료기기의 사이버보안(2019년 7월)

23. 중국: 기술 검토 지침 원칙에 따른 의료기기 네트워크 보안 등록(2017년 1월)

24. 유럽 위원회: 지침 2001/83/EC, 지침(EC) No 178/2002 및 규정(EC) No 1223/2009의 개정본, 위원회 지침 90/385/EEC 및 93/42/EEC 폐지, 의료기기에 관한 2017년 4월 5일자 유럽 의회 및 위원회의 규정(EU)(2017년 5월)

25. 유럽 위원회: 지침 98/79/EC 및 위원회 결정 2010/227/EU 폐지, 체외진단 의료기기에 관한 2017년 4월 5일자 유럽 의회 및 위원회의 규정(EU) 2017/746(2017년 5월)

26. FDA(초안): 의료기기 사이버보안 관리를 위한 시판 전 제출서 내용(2018년 10월)

27. FDA: 상용 소프트웨어(OTS: Off-the-Shelf)를 포함하는 네트워크 의료기기의 사이버보안(2005년 1월)

28. FDA: 가정용 기기의 설계 고려 사항(2014년 11월)

29. FDA: 의료기기의 사이버보안에 대한 시판 후 관리(2016년 12월)

30. 독일: 네트워크 연결 의료기기의 사이버보안 요구 사항(2018년 11월)

31. 캐나다 보건부: 의료기기 사이버보안에 대한 시판 전 요구 사항(2019년 6월)

32. 일본: 의료기기의 사이버보안 보장: PFSB/ELD/OMDE Notification No. 0428-1(2015년 4월)

33. 일본: 의료기기의 사이버보안 보장 지침: PSEHB/MDED-PSD Notification No. 0724-1(2018년 7월)

34. 싱가포르 표준 위원회 기술 참고 문헌 67: 의료기기 사이버보안(2018)

35. TGA: 의료기기 사이버보안 - 소비자 정보(2019년 7월)

36. TGA: 산업용 의료기기 사이버보안 지침(2019년 7월)

37. TGA: 사용자용 의료기기 사이버보안 정보(2019년 7월)

7.4 기타 자원 및 참고 자료

38. 조정된 취약점 공개에 대한 CERT 지침
https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

39. NIST 사이버보안 프레임워크
https://www.nist.gov/cyberframework

40. NIST 시큐어 소프트웨어 개발 프레임워크(SSDF: Secure Software

Development Framework)
https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

41. 의료기기 및 보건 IT 공동 보안 계획(2019년 1월)
https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

42. MITRE 의료기기 사이버보안 플레이북(2018년 10월)
https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

43. MITRE CVSS 의료 지시문
https://www.mitre.org/publications/technical-papers/rubric-for-applying-cvss-to-medical-devices

44. Health Industry Cybersecurity Practices: 보건 산업 사이버보안 실무: 위협 관리 및 환자 보호(HICP)
https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

45. 오픈 웹 애플리케이션 보안 프로젝트(OWASP: Open Web Application Security Project)

https://www.owasp.org/index.php/Main_Page

46. 의료기기 보안을 위한 제조업체 공개 진술서(MDS^2 : Manufacturer Disclosure Statement for Medical Device Security) https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

47. NIST 프레임워크를 의료기기에 적용하는 ECRI 접근 방식 https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical-Devices.aspx

48. TIA/미 상무부, 취약점 공개 태도 및 조치: NTIA 인식 및 채택 그룹 연구 보고 https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf

49. https://republicans-energycommerce.house.gov/wp-content/uploads/2018/10/10-23-18-CoDis-White-Paper.pdf

50. https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

8.0 부록

8.1 부록 A: 사고 대응 역할(ISO/IEC 27035)

사고 관리 – ISO/IEC 27035		
계획 및 대비	정보 보안 사고 관리 정책을 수립하고 사고 대응 팀을 구성하는 등의 작업 수행	
감지 및 보고	누군가 사고이거나 사고로 이어질 수 있는 '사건'을 발견하고 보고해야 함	
평가 및 결정	누군가 해당 상황을 평가하여 실제 사고 여부를 결정해야 함	
대응	해당하는 경우, 사고를 억제, 근절하고, 사고를 복구하고 법의학적으로 분석	
교훈	사고 경험의 결과를 바탕으로 조직의 정보 위험 관리를 체계적으로 개선	
사고 대응 팀		
역할	**담당 책임**	**주요 조치**
관리자	사이버 보안 사고 대응 관련 주요 문제에 관한 의사결정 주도	a) 필요한 자원(인력, 재정, 물질)의 제공을 포함한 사고 대응에 대한 약속과 지원 b) 사고 대응 정책 및 계획을 검토, 승인하고, 해당 이행을 감독 c) 사고 대응 계획에 대한 검토 및 승인 d) 팀의 내부 및 외부 조정
계획 그룹	사고 대응 운영	a) 보안 정책 수립 및 계획 b) 보안 절차 실행 c) 위험 우선순위 조정 d) 상위 조직 및 기타 서드파티 조직과의 의사소통 e) 관리 지원 f) 대상 조직에 관한 취약점 보고서를 논의/등록/승인 g) 관리자가 지시한 기타 활동 수행

사고 대응 팀		
역할	**담당 책임**	**주요 조치**
모니터링 그룹	모니터링 그룹	a) 모니터링 및 작전 매일 수행 b) 침입 감지, 사고 등록, 최초 대응 c) 보안 업데이트 수행 d) 보안 정책 및 백업 관리 실행 E) 컴퓨터 관련 업무 지원 센터 f) 시설 관리 g) 관리자가 지시한 기타 활동 수행
대응 그룹	실시간 대응, 기술 지원과 같은 서비스 제공	a) 사고 관련 정보 전파 및 보고 b) 모니터링 시스템 간의 상관관계 분석 c) 사고 조사 및 복구 지원 d) 대상 사고 관련 취약점 분석 e) 관리자가 지시한 기타 활동 수행
실행 그룹	총체적 사고 대응 조치 수행	a) 사고 대응 요구 사항 분석 b) 사고 대응 정책 및 수준 결정 c) 사고 대응 정책 및 계획의 실행 d) 사고 대응 계획 예상 e) 사고 대응 작업 및 보고서 요약 f) 사고 대응 자원 배치 및 사용 g) 관리자가 지시한 기타 활동 수행
분석 그룹	사고 분석 수행	a) 팀과 제조업체의 취약점 분석 계획 b) 보안 분석 도구 및 체크리스트 개선 c) 모니터링 규칙 개선 d) 뉴스레터 발행 e) 관리자가 지시한 기타 활동 수행

8.2 부록 B: 조정된 취약점 공개에 관한 관할 구역별 자원

호주

호주 CERT

https://www.cert.gov.au/

AusCERT

https://www.auscert.org.au/

브라질

브라질 CERT

https://www.cert.br/csirts/brazil/

캐나다

캐나다 사이버 보안 센터(Canadian Centre for Cyber Security)

https://www.cyber.gc.ca/

유럽

유럽 연합 CERT

https://cert.europa.eu

프랑스

ANSM

https://ansm.sante.fr/

https://www.ansm.sante.fr/Declarer-un-effet-indesirable/Votre-declaration-concerne-un-dispositif-medical/Votre-declaration-concerne-un-dispositif-medical/(offset)/0

프랑스 보건 및 연대부(French Ministry of Health and Solidarity)
https://solidarites-sante.gouv.fr/soins-et-maladies/signalement-sante-gouv-fr/

공유 건강 정보 시스템 기관(Shared Health Information Systems Agency)
https://www.cyberveille-sante.gouv.fr/

국가 정보 시스템 보안국(ANSSI - National Agency for Information Systems Security)
https://www.ssi.gouv.fr/en/

독일

독일 CERT
https://www.cert-bund.de/

이탈리아

https://www.csirt-ita.it/

일본

일본 컴퓨터 비상 대응 팀/조정 센터(JPCERT/CC: Japan Computer Emergency Response Team/Coordination Center)

https://www.jpcert.or.jp/vh/top.html또는 https://www.jpcert.or.jp/english/

싱가포르

SingCERT

https://www.csa.gov.sg/singcert/news/advisories-alerts

미국

산업 제어 시스템 CERT(ICS-CERT)

https://www.us-cert.gov/ics

미국 CERT

https://www.us-cert.gov/