MEDIDATA

백서

정보 보안

목차

임원용 요약

Medidata는 효과적인 정보 보안 및 사이버 방어 프로그램이, 제품의 설계, 개발, 생산, 유통, 배포, 유지관리, 처분, 및 그 관련 데이터를 포함하여, 전체 제품 수명 주기를 반드시 다루어야 한다는 것을 인식하고 있습니다.

Medidata는 모든 Medidata 제품이 Medidata 사용 지침에 따라 사용된다는 조건하에, 그러한 제품과 관련된 보안 사고 및 개인정보 침해로부터 보호를 돕기 위해, 행정적, 기술적, 및 물리적 안전장치를 시행하고 있습니다. 그러나, 시스템 및 위협이 진화함에 따라, 모든 위협 및 취약점으로부터 보호할 수 있는 시스템은 없습니다. 앞을 내다보는 전략과 지속적인 평가는 합리적인 방어 프로그램의 핵심 구성요소입니다. 당사의 고객은 중요하며 당사는 관리되는 모든 데이터 및 서비스의 보안 및 개인정보 안전장치를 유지관리하기 위해 귀하와 협력하고 있습니다.

귀하가 우려사항이 있는 경우, 당사에 알려주시면, 당사는 조사할 것입니다. 적절한 경우, 당사는 제품 변경, 기술 공지, 및/또는 고객과 규제기관에 대한 책임 있는 공개를 통해 문제를 해결할 것입니다. Medidata는 다음과 같은 관행을 사용하여 제품 수명 주기 전반에 걸쳐 보안 및 개인정보를 개선하기 위해 지속적으로 노력하고 있습니다: 설계를 통한 개인정보 및 보안, 제품 및 공급업체 리스크 평가, 취약점 및 패치 관리, 자동화된 취약점 스캐닝, 외부 제3자 테스트, 고객 액세스 및 데이터에 적절한 액세스 관리, 및 사고 대응.

"정보 보안은 환자 개인정보 및 경우에 따라 환자의 생명 보호에 중요합니다; 제가 임상시험 환자가 되었을 때, 의료 데이터 보호는 개인적인 것이 되었습니다. 임상시험 환자이자 사이버 위협을 이해하는 보안 전문가로서, 저는 Medidata는 제가 정보를 저장하고 처리하고 싶은 유일한 회사라고 말할 수 있습니다."

- Glenn Watt, Medidata, 최고 정보 보안 책임자(2007-2018)

Medidata는 당사의 고객을 위해 최선을 다하고 있으며, 당사는 고객이 당사 제품 및 서비스에 대한 질문, 우려사항, 및 개선사항에 대해 당사에 연락하도록 권장합니다.

질문이 있거나 명확한 설명이 필요한 경우, 언제든지 Medidata.asksecurity@3ds.com으로 연락하십시오.

목적

본 문서의 목적은 Medidata 보안 및 개인정보 관행이 Medidata Clinical Cloud (MCC)에 어떻게 적용되었는지에 대한 공개적으로 이용 가능한 정보에 대해 논의하는 것입니다. 여기에는 Medidata가 제품의 각 보안 영역을 유지하는 방법 및 제품 수명 주기 전반에 걸쳐 보안을 보장하기 위해 귀하와 협력할 수 있는 방법을 기술하는 설명이 수록되어 있습니다.

당사는 기밀 또는 독점 보안 제품 이름, 구성, 및 운영 절차는 공개하지 않으면서, 귀하에게 Medidata 보안 문제 및 답변에 대한 일반적인 논의를 제공하고자 합니다. 이러한 관행 및 기술은 고지 및 문서 업데이트 없이 업데이트될 수 있으므로, 본 문서의 어떤 부분도 계약상의 의무를 충족하는 것으로 간주되어서는 안 됩니다.

보다 자세한 기밀 문의가 있을 경우, 귀하의 Medidata 연락 담당자/세일즈 엔지니어/전문 서비스/고객 담당 임원에게 문의하십시오.

Medidata 보안 문화

조직의 모든 구성원이 공유하는 가치에 따라 사람들이 보안에 대해 생각하고 접근하는 방식이 결정됩니다. 강건한 보안 문화를 구축하면 보안 의식이 있는 인력을 양성하고 직원들에게 필요한 보안 행동을 장려할 수 있습니다. 이를 "인간 방화벽"이라고 합니다. Medidata 및 파트너사 모두의 직원들은, 어떤 것이 평범하지 않고 의심스러운지 '알고' 있습니다. 개인적인 경험 및 관찰은 자동화될 수 없습니다. 이는 당사가 구매하고 배포하는 도구의 한계입니다.

Medidata는 "보안 설계"라는 사고방식을 가지고 제품을 개발합니다. 오픈 월드와이드 애플리케이션 보안 프로젝트(Open Worldwide Application Security Project, OWASP) 소프트웨어 개발 원칙은 엔터프라이즈 기술 아키텍처의 설계 및 수정뿐만 아니라, 소프트웨어 개발 수명 주기(Software Development Life Cycle, SDLC)에 대한 핵심 전략을 수립합니다.

OWASP 보안 설계 원칙은 다음과 같습니다:

- **공격 표면 영역 최소화하기 –** 사용자에게 필요한 기능만 제공하도록 축소함
- **보안 기본값 설정하기 –** 강력한 보안 규칙으로 사용자 및 사용자의 액세스를 관리함
- **최소 권한 원칙 –** 사용자는 특정 작업을 수행하는 데 필요한 최소한의 권한만 가져야 함
- **심층 방어하기 –** 제품은 반드시 여러 계층의 검증, 추가 보안 감사 도구 및 로깅이 있어야 함
- **안전하게 실패하기 –** 오작동하는 프로그램은 기본적으로 액세스 권한이 적거나 없어야 함
- **서비스 신뢰하지 않기 –** 프로그램 내에서 활용되는 제3자 소프트웨어 및 서비스에 상위 수준의 권한을 부여해서는 안 되며 데이터 반드시 스트림이 검증되어야 함
- **업무 분리 –** 개인의 부정 행위를 방지함
- **모호함에 의한 보안 문제 방지하기 –** 충분한 보안 제어 기능을 사용하여 핵심 기능이나 소스 코드를 숨기지 않고 애플리케이션을 안전하게 유지함
- **보안을 단순하게 유지하기 –** 가능한 경우 복잡성을 줄여 코드가 잘 보이도록 함
- **보안 문제를 올바르게 해결하기 –** 반드시 결함에 대한 근본 원인 분석을 수행한 후 조치를 취해야 함

정보 보안은 Medidata 비즈니스 문화의 일부이기도 합니다. Medidata의 정보 보안 거버넌스 구축 전략에는 고객 데이터의 기밀성, 무결성, 및 가용성을 유지하여, 랜섬웨어나 데이터 침해와 같은 악의적인 사건으로 인한, 비즈니스 피해 가능성을 최소화하는 것이 포함됩니다.

Medidata의 거버넌스 전략은 업계 최고의 훈련 및 교육을 결합하여 구현되며, 보안 운영, 보안 엔지니어링, 보안 아키텍처, 사고 대응, ID 및 액세스 관리, 리스크 관리 및 보안 프레임워크를 포함한, 전문화된 기능을 중심으로 구성된 고도로 숙련되고 인증을 받은 보안 전문가로 구성된 다양한 팀이 협력 및 지원합니다. Medidata의 보안 거버넌스 구현은 Medidata가 모든 적절한 보안 및 개인정보 요건을 준수하도록 보장하기 위해 최소 매년 테스트하고 감사합니다.

기업 리스크 관리

Medidata의 집행위원회(Executive Committee, XCOM)는 고객에 대한 책임을 다하려면 강력한 통제 구조가 필요하다는 점을 인식하고 있습니다. 따라서, 효과적인 보안 제어를 갖추도록 보장하려는 노력은 Medidata의 전반적인 리스크 관리 전략의 필수적인 부분입니다.

최고 정보 보안 책임자(Chief Information Security Officer, CISO)가 감독하는, 이 프로세스는 전략적 감독의 결과를 활용하여 전략적 리스크 등록부를 작성합니다. 이 리스크 등록부는 운영상 식별된 위협 및 새로 나타나는 글로벌 사이버 보안 위협뿐만 아니라, 보안 요건 및 제어에 대한 높은 수준의 관점을 통합합니다.

이러한 리스크 및 그에 대한 대처는 Dassault Systèmes 이사회 업데이트의 일부입니다. 당사는 조직의 전략적 프로그램으로서 하향식 지원을 계속 받고 있습니다.

미래 지향적인 조직은 리스크가 모두의 비즈니스라는 것을 알고 있습니다. 이는 하나의 비즈니스 라인에 국한되거나 독립적으로 또는 서로 분리되어 운영되는 회사 내 조직 구조 또는 부서 내에서 임시로 수행될 수 없습니다. 리스크의 소유권은 반드시 전사적으로 공유되어야 하고, 긴밀하게 협력하고 투명해야 합니다. Medidata는 현재 글로벌 시장의 변동성 및 지난 몇 년간 경제, 비즈니스, 사회 생태계가 크게 혼란을 겪으면서 힘들게 얻은 교훈을 고려하여, 이것이 사실임을 알고 있습니다.

이상적인 세계에서는—사이버, 비즈니스, 운영, 평판을 포함하여—이러한 혼란 및 리스크를 효과적으로 관리하고 완화하는 데 필요한 실시간 정보가 회사로 유입되어, 함께 일하면서 충분한 정보를 바탕으로 신속하게 의사 결정을 내릴 수 있는 권한을 가진 잘 정의된 이해관계자 그룹 전반에 공유될 것입니다.

우리가 예측할 수 없고 빠르게 변화하는 세상과 그 결과로 현실화된 확장되는 위협 환경을 성공적으로 헤쳐나가야 한다면, Medidata는 여기 있는 우리 모두가 노력해야 할 목표인 이 이상적인 상태를 열망합니다.

Medidata에서의 성공은, 잠재적 리스크 사건이 전개됨에 따라, 이를 실시간으로 탐지하는 데 필요한 시스템 및 프로세스를 활용하는, 사전 예방적 통합 보안 및 리스크 관리 솔루션을 구축하는 데 기반을 두고 있습니다.

정보 보안 프레임워크 및 감사

Medidata는 일반 데이터 보호 규정(General Data Protection Regulation, GDPR) 및 기타 현지 규정도 준수뿐만 아니라, 국제표준화기구(International Organization Standardization, ISO) 27001, 27002, 27701, 27017 및 27018, SOC1 및 SOC2+ , 및 NIST 800-53v5를 포함하는, 여러 인증의 보안 프레임워크, 보안 제어, 및 보안 방법을 구현합니다. 당사는 또한 미국 연방 고객을 위해 미국 연방정보보안관리법(Federal Information Security Management Act, FISMA) 중간 수준의 운영 권한도 보유하고 있습니다. 인증된 제3자가 수행하는 외부 감사는 ISO, FISMA 및 SOC2+ 에 대해 매년 수행되며, 귀하의 제품, 소프트웨어, 또는 서비스를 제공하고 지원하는, Medidata 인력, 프로세스, 및 기술에 대한 관련 세부 사항을 다룹니다.

각 인증 감사는 Medidata의 현재 및 잠재 고객에게 Medidata가 지역적, 국가적, 및 국제적 법률 및 규정을 준수한다는 확신을 제공합니다. 각 감사는 외부 감사인을 통해 수행되며, 모든 발견 사항 또는 규정 미준수 사항은 Medidata 티켓팅 시스템에서 추적됩니다. 이러한 티켓은 근본 원인에 대한 세부 정보를 포함하고 있으며, 문제 해결에 필요한 노력과 함께 정기적으로 업데이트되어야 합니다. 필요에 따라, 검토 및 상부 보고를 위해 월별 보고서가 정보 보안 경영진에게 전달됩니다.

Medidata는 이러한 보안 프레임워크에서 정한 규범적 요건을 기반으로 “동급 최고의” 하이브리드 솔루션(조직적 및 기술적)을 사용합니다. 이러한 총체적인 접근 방식은 정해진 모든 요건을 충족하는 보안 제어 및 메커니즘의 포괄적인 구현을 지원합니다.

경계 확보 및 보호

Medidata의 액세스 제어 구현은 모든 계정을 지속적으로 관리하고, 할당된 사용자의 역할과 책임에 따라 권한이 있는 계정과 권한이 없는 계정 모두에 대한 액세스를 제한하고 최소화하도록 설계되었습니다. 액세스 관리 요건은 모든 계정에 대한 액세스 추가/제거/변경 지침을 제공하고, 제한된 액세스를 시행하기 위한 제어 시스템을 식별하며, 부여된 모든 액세스 권한의 검토 빈도를 파악하는 데 사용됩니다. 필요한 경우 계정을 자동으로 비활성화하고 모든 계정 관리 활동(계정 생성, 수정, 활성화, 비활성화, 및 삭제)을 감사하는 것을 포함하여, 다양한 자동화된 도구를 지속적으로 사용하여 계정 관리를 시행합니다.

사전 승인된 상호 연결은 확립된 서비스 수준 계약에 따라 시스템 내에서 정보 흐름이 시행되도록 하는 데 사용됩니다. Medidata는 모든 요청이 티켓팅 시스템에서 관리되는 계정 처리 활동을 조정하기 위해 최소 두 명의 관리자를 요구합니다. 계정은 ID 액세스 관리 팀에서 분기별로 검토됩니다. 실패한 로그인 시도 제한 및 잠금 자가 복구는 CIS 벤치마크에서 설정한 지침에 따라 시행됩니다. 식별 및 인증 없이는 사용자 또는 기기의 어떠한 작업도 허용되지 않습니다. 원격 액세스는 모든 연결에 대해 MFA 및 암호화를 통해 시행됩니다. 모든 계정 액세스는 보안 사건 및 사고 관리자와 게이트웨이 보호 방법을 통해 모니터링됩니다.

ID 제공자 및 서비스(Identity Provider and Services, IdP IpS)

Medidata는 Medidata 시스템 액세스를 위해 ID 제공자(약칭 IdP 또는 IDP)를 사용하여, 주체에 대한 ID 정보를 생성, 유지 및 관리하고, 연방 또는 분산 네트워크 내에서 의존적 애플리케이션에 인증 서비스도 제공합니다.

당사는 신뢰할 수 있는 IDP를 사용하여 애플리케이션에 대한 액세스를 관리할 수 있도록 사용자 인증을 서비스로 제공합니다. ID 제공자는 다른 웹사이트에 액세스할 때 싱글사인온(single sign-on, SSO)을 사용할 수 있도록 해주는 신뢰할 수 있는 제공자로, 비밀번호의 피로감을 줄여 사용성을 향상시키고 잠재적인 공격 표면을 줄여 보안을 강화합니다.

ID 제공자는 클라우드 컴퓨팅 리소스와 사용자 간의 연결을 촉진하여, 모바일 및 로밍 애플리케이션을 사용할 때, 사용자가 재인증할 필요성을 줄일 수 있습니다.

최소 권한 기능은 CIS 벤치마크 구성 설정을 준수하고 다양한 호스트 및 게이트웨이 액세스 제한을 적용하여 구현됩니다.

식별, 인증, 및 권한

Medidata는 ISO 및 NIST에서 정한 요건에 부합하는 식별 및 인증 방법을 구현합니다. Medidata 직원 및 고객 사용자를 포함한, 모든 사용자는 고유한 ID를 사용하여 인증됩니다. 사용자 계정 및 비밀번호는 자격 증명의 공유가 허용되지 않는 사용자 고유의 것이어야 합니다. Medidata는 또한 모든 직원에게 다단계 인증을 시행하고 있으며 고객에게 선택 사항으로 다단계 인증을 제공합니다.

MCC는 액세스 및 권한 제어, 포괄적인 감사 추적, 전자 서명을 전자 기록에 연결하여 부인 방지를 확립하는 전자 서명 시스템을 제공합니다. Medidata는 사용자 계정을 활성화할 때와 운영을 관리 및 지원할 때, 고객과 직원이 이러한 요건을 이해하고 서명하도록 요구합니다.

사이버 보안 및 정보 보안 인식 교육

Medidata의 사이버 보안 교육 시행은 계약업체를 포함한 모든 직원이, 자신의 직책 및 보안 책임에 맞는 적절한 교육을 받도록 하기 위해 설계되었습니다.

Medidata 전체에서 여러 표적화된 교육 모듈이 사용됩니다. 연간 교육은 추적되며, 교육 과정을 이수하지 않은 직원 또는 계약업체는 모든 Medidata 시스템에서 액세스 권한이 박탈됩니다. 영구 복직하려면 교육을 이수하고 관리자의 승인을 받아야 합니다.

교육은 Medidata의 학습 관리 시스템을 통한 이러닝 교육 과정을 통해 관리되며, 3DS 학습 관리 시스템 내에서 온디맨드 방식으로 추가 과정도 이용할 수 있습니다.

감사 또는 모니터링

Medidata의 보안 사건 감사 구현은 필요한 모든 감사 대상 사건이 수집되고 ISO 27001 제품군 및 NIST 800-53 요건과 일치하도록 설계되었습니다. Medidata는 보안 위반, 침입 시도, 무결성 사건, 시스템 및 구성요소 장애, 및 사용자 활동 사건에 대한 감사를 포함하는, 이러한 요건을 모니터링하고, 이에 대해 감사하기 위해 다양한 보안 정보 및 사건 관리(Security Information and Event Management, SIEM) 도구를 사용합니다. 감사 가능한 모든 사건은 지속적으로 모니터링됩니다.

SIEM

보안 정보 및 사건 관리(SIEM) 기능이 전체 환경에 걸쳐 구현됩니다. 시스템 전체에서 미연방 정보처리 표준(Federal Information Processing Standard, FIPS) 140-2를 준수하는 암호화 방법 및 솔루션이 사용됩니다.

구성 관리

Medidata는 다양한 구성 변경 관리 도구, 프로세스, 및 절차를 사용하여, 모든 시스템 및 구성요소의 수명 주기 전반에 걸쳐 구성 관리를 구현합니다. 기본 구성은 자동화된 도구에서 지원하는 검증 패키지로 유지관리됩니다. 모든 변경사항은 체계적으로 추적됩니다. 테스트 및 검증은 구성 관리 프로세스의 필수적인 부분입니다. 보안 및 개인정보 담당자는 변경 심사위원회(Change Review Board, CRB)의 위원이며 적절한 경우 보안 및 개인정보 리스크 평가를 제공합니다.

비즈니스 연속성 및 재해 복구(BC/DR)

Medidata는 조직 전체에 적용되는 포괄적인 비즈니스 연속성 및 재해 복구(Business Continuity and Disaster Recovery, BC/DR) 기능을 구현합니다.

계획 프로세스는 Medidata 자체의 요구뿐만 아니라 서비스 수준 협약(Service Level Agreement, SLA)에 표현된 고객의 요구사항에 따라 추진됩니다. 서비스 제공, 고객 성공, 및 전문 서비스 팀을 포함하는, Medidata 내 모든 주요 개인 및 조직이 연례 재해 복구 계획 연습 및 검토에 참여합니다. 당사의 계획 프로세스에는 고객 SLA에서 설정한 복구 시간 목표 내에서 모든 미션 및 비즈니스 기능을 복구하는 것이 포함됩니다. 이 계획 프로세스 동안 모든 미션 및 비즈니스 기능뿐만 아니라 모든 중요 시스템 자산을 식별합니다. 그에 따라 세워진 계획은 최소 매년 한 번 이상 테스트를 거쳐 피드백 및 테스트 결과를 바탕으로 지속적으로 기능을 개선합니다.

사고 대응 및 처리

Medidata는 시스템 및 데이터의 기밀성, 무결성 및 가용성에 대한 즉각적인 위협을 신속하게 식별, 억제 및 교정할 수 있는 포괄적인 사고 대응 계획을 유지합니다.

Medidata는 24시간 연중무휴 전담 보안 운영팀인 글로벌 네트워크 운영 센터(Global Network Operations Center, G-NOC)를 유지관리하여, 모든 사고 처리 활동을 모니터링하고 지원합니다. Medidata의 보안 운영팀은 SIEM과 다양한 로깅 및 사건 관리, 보고 도구를 포함한 다양한 자동화된 사고 관리 도구를 사용합니다. 정보 보안 경고는 보안 운영 센터(Security Operations Center, SOC) 또는 글로벌 네트워크 운영 센터(GNOC) 시스템에서 정보 보안 직원에게 상부 보고된 후, 연구개발(Research and Development, R&D)(정보 보안[Information Security, InfoSec]) 담당 부사장 및 고위 경영진에게 전달됩니다. 당사의 사고 대응 프레임워크는 고객 알림을 촉발할 수 있는 상황과 고객에게 정보를 제공하는 방법을 자세히 설명합니다. 이 정책은 또한 보안 사고의 수명 주기를 제어하기 위한 대응을 참조합니다. 이 계획은 사건 및/또는 사고의 식별, 준비, 억제부터 복구, 알림, 사후 조치에 이르기까지, 그러한 단계 및 해당 단계와 관련된 조치에 대해 설명합니다. Medidata는 탐지 후 합리적인 시간 내에 보안 사고의 영향 분석을 확인하고 수행한 후, 서비스 계약에 명시된 커뮤니케이션 채널을 통해 Medidata 고객에게 알립니다. 모든 문제는 온라인 데이터베이스 기반 문제 관리 시스템에서 추적됩니다. Medidata는 사고 대응 교육 및 테스트를 연례 재해 복구 테스트에 통합합니다.

유지관리

Medidata는 모든 보안 보호 기능을 완벽하게 온전한 상태로 유지하는 것을 전반적인 목적으로 하여 이루어진, 모든 변경사항에 대한 우선순위 지정 및 승인 요건을 포함하는, 엄격한 유지관리 프로그램을 구현합니다. 취약점 스캐닝, 애플리케이션 스캐닝 및 멀웨어 보호 조치를 시행하여, 유지관리 활동 중에 사용되는 모든 매체를 점검합니다. 외부 장치는 먼저 스캔하지 않고는 연결할 수 없으며, 운영 직원의 통제 하에 있을 때만 연결할 수 있습니다. 모든 유지관리는 변경 관리 프로세스의 일부로 문서화되고 허가되며, 롤백 계획과 테스트 및 검증 요건을 포함합니다.

매체 보호

Medidata는 데이터가 처리되거나 저장되는 각 위치에서 매체 보호를 시행합니다. 모든 데이터는 운영 직원이 액세스 권한을 관리하는 제한된 액세스 데이터로 취급됩니다. 여기에는 데이터의 파기, 제거, 백업, 및 복구를 위한 액세스 권한이 포함됩니다. 파기하도록 지정된 모든 매체는 추적되며 파기된 각 매체에 대한 파기 인증서가 생성됩니다. 매체는 Medidata 외부에서 절대 재사용되지 않습니다. 사용 중이거나 전송 중이거나 저장 중인 모든 매체는, 데이터 무결성 및 기밀성을 유지하기 위해, FIPS 140-2를 준수하는 암호화 방법을 사용하여 보호됩니다.

데이터 손실 방지

Medidata에서 데이터 손실 방지(Data Loss Prevention, DLP)는 민감한 데이터가 손실되거나 오용되거나 권한이 없는 사용자가 액세스하는 것을 방지하는 데 사용되는 일련의 도구 및 프로세스입니다. DLP 소프트웨어는 규제 대상, 기밀 및 비즈니스에 중요한 데이터를 분류하고, 조직에서 정의한 정책 또는 사전 정의된 정책 팩 내에서 정책의 위반을 식별하며, 이는 일반적으로 HIPAA 또는 GDPR과 같은 규제 준수에 의해 구동됩니다. 이러한 위반이 확인되면, DLP는 경고, 암호화, 및 기타 보호 조치를 통해 교정을 시행하여, 최종 사용자가 실수로 또는 악의적으로 조직을 리스크에 빠뜨릴 수 있는 데이터를 공유하지 못하도록 합니다. 데이터 손실 방지 소프트웨어 및 도구는 엔드포인트 활동을 모니터링 및 제어하고, 기업 네트워크의 데이터 스트림을 필터링하며, 클라우드의 데이터를 모니터링하여 저장 중, 이동 중, 및 사용 중인 데이터를 보호합니다. DLP는 또한 규정 준수 및 감사 요건을 충족하고 포렌식 및 사고 대응을 위한 취약 및 이상 영역을 식별하기 위한 보고 기능을 제공합니다.

환경 보안

권한이 있는 직원으로 제한되는 시설 및 보호 대상 정보 자산에 대한 물리적 액세스. Medidata는 정보 시스템이 포함된 시설에 대한 접근 권한이 있는 직원의 최신 목록을 유지하고 적절한 허가 자격증명(예: 배지, 신분증, 스마트카드)을 발급합니다. 조직 내 지정된 담당자는 적어도 매년 액세스 목록 및 권한 부여 자격증명을 검토하고 승인합니다.

설계상 공개적으로 액세스할 수 있는 영역은 없습니다. 물리적 액세스 목록은 건물 관리인이 관리하지만 시설 보안팀에서 주기적으로 검토합니다. 데이터 센터에 액세스하려면 생체 인식, 스마트카드, 및 PIN 코드의 조합이 적절한 순서로 필요합니다. 에스코트 없는 출입이 제공되기 전에 액세스 목록에 추가하려면 반드시 고위 경영진의 승인을 받아야 합니다.

Medidata는 정보 시스템에 대한 물리적 액세스를 모니터링하여 물리적 보안 사고를 탐지하고 대응합니다. 물리적 액세스는 자동으로 기록되며 검토에 이용할 수 있습니다. 카메라는 물리적 접근을 기록하는 데 사용됩니다.

Medidata는 시설에 대한 접근을 허가하기 전에 방문자를 인증하여 정보 시스템에 대한 물리적 접근을 통제합니다. 방문자가 액세스하려면 먼저 액세스 요청을 하고 해당 Medidata 직원의 승인을 받아야 합니다. 모든 방문객은 시설 내에서 에스코트를 받습니다.

Medidata는 보안 구역 및 장비의 물리적 보안에 대한 문서화된 절차를 동반한 공식적인 정보 보안 정책을 유지합니다.

보안 계획

Medidata는 ISO 27001에 기반한 지속적인 보안 프로그램 개선 프로세스를 시행합니다. Medidata Clinical Cloud를 위해 NIST를 준수하는 시스템 보안 계획과 함께 ISO 27001 인증을 받은 정보 보안 관리 시스템이 구현되었습니다. 이러한 계획은 매년 업데이트되어 새롭게 변화하는 보안 및 개인정보 아키텍처 요건을 통합하고 강력한 Medidata 보안 기능을 보장합니다. 이 접근 방식은 모든 보안 및 개인정보 아키텍처 변경사항이 보안 계획, 적격성평가 문서, 엔지니어링 문서, 제품 문서, 및 호스팅 문서에 통합되도록 합니다.

인적 보안 – 인적 자본

직원은 신원 조회 절차에 따라 수행된 신원 조회 결과를 고려하여 인력 행동 기준에 따라 고용됩니다. 모든 직원은 Medidata 시스템에 대한 액세스 권한을 부여받기 전에, 비즈니스 행동 강령을 읽고 숙지하고 준수해야 합니다. 이 과정을 완료하면 Medidata의 학습 관리 시스템에 수집됩니다. 이러한 인적 보안 프로세스는 제3자 계약업체 및 컨설턴트에게도 적용됩니다.

제품 및 서비스 적격성평가

Medidata는 매년 계획, 문서화, 및 승인되고, 보안 및 개인정보 요건에 대한 고려를 포함하는 포괄적인 획득 프로세스를 구현합니다. 여기에는 모의 해킹, FISMA 평가, ISO 감사, SOC2 감사, 유럽연합(European Union, EU)-미국(United States, US) 데이터 개인정보 프레임워크(Data Privacy Framework, DPF) 인증 및 기타 보안 관련 활동에 대한 자금 지원이 포함됩니다. 또한 새로운 보안 및 개인정보 기능을 시스템 소프트웨어에 통합하는 데 필요한 암호화 제품 및 소프트웨어에 대한 자금 지원도 계획에 포함되어 있습니다. 정보 보안 및 개인정보 팀은 획득 프로세스에 참여하여 획득 중 모든 보안 및 개인정보 요건이 고려되도록 합니다.

시스템 및 정보 무결성

Medidata는 자동화된 도구, 티켓팅 시스템, 패치 관리 시스템, 품질 보증 프로세스를 사용하여, 조직 전체에 시스템 및 정보 무결성 보증을 구현하고, Medidata 시스템의 수명 주기 전반에 걸쳐 발견사항을 모니터링, 스캔, 및 교정하기 위한 품질 보증 프로세스를 구현합니다. 악성 코드 보호는 전사적으로 적용될 때 중앙에서 모니터링 및 관리됩니다. 무결성 모니터링 도구는 환경 전반에 걸쳐 Medidata 시스템의 무결성을 보장하기 위해 사용됩니다. Medidata 시스템 내의 정보는 저장 및 전송 중 암호화되어 있습니다. 또한, Medidata는 국가 취약점 데이터베이스를 지속적으로 모니터링합니다.

제3자 리스크 관리(Third Party Risk Management, TPRM)

Medidata는 개인정보(Personally Identifiable Information, PII)를 포함하여 서비스 제공의 일환으로 Medidata를 대신하여 데이터에 액세스하고 데이터를 처리하는 제3자 및 하위 서비스 제공자를 이용합니다.

Medidata 개인정보 사무소(Medidata Privacy Office, MPO)는 비즈니스 영역, 주제 전문가 및 관리 부서와 협력하여, 참여자의 개인정보 처리와 관련된 제3자의 필수 개인정보 약속을 설명하는 조항이 포함된 계약서를 개발합니다. MPO 및 법무팀은 Medidata 표준에 따라 개인정보 관련 조항이 포함되어 있는지 검증하기 위해 새로운 제3자 계약을 검토하고 승인합니다.

글로벌 규정 준수 및 전략(Global Compliance & Strategy, GCS)은 MPO, 정보 보안(InfoSec) 및 비즈니스 영역과 협력하여, 모든 신규 벤더가 Medidata 시스템 및 환경에 액세스하는 제3자 벤더에 대해 정의된 리스크 기반 평가를 받도록 합니다. Medidata는 참여자의 개인정보(PII)를 액세스, 사용 및/또는 저장하는 벤더를 우선순위로 하여 제3자 벤더에 대한 주기적인 리스크 평가를 실시하고 결과를 분석하며, 필요하다고 판단되는 경우, 리스크 평가 결과 리스크가 더 높은 것으로 간주되는 제3자 벤더를 평가하기 위한 문서화된 계획을 수립합니다. 벤더 평가는 정의된 Medidata 공급업체 평가 정책 및 절차에 따라 수행됩니다. 벤더 평가 결과는 문서화됩니다.

공급업체 평가 및 감사

Medidata SDLC를 지원하거나 Medidata, Medidata 고객 또는 Medidata 파트너에게 서비스를 제공하기 위해 제안된 모든 제3자 벤더는 Medidata 직원의 보안 평가 대상입니다. Medidata는 초기에 및 주기적으로 공급업체를 평가하여 기본적인 운영 보안 지표가 Medidata의 요건을 충족하고 있는지 확인합니다. 공급업체는 주기적으로 평가를 받습니다: 중요 공급업체는 마지막 평가 후 12개월 이내에 평가를 받고, 주요 공급업체는 마지막 평가 후 12~24개월 이내에 평가를 받으며, 소규모 공급업체는 마지막 평가 후 24~36개월 이내에 평가를 받습니다.

공급업체 감사 및/또는 설문조사는, 감사 및/또는 설문조사 빈도와 관계없이, 공급업체와 관련된 예기치 않은 사건으로 인해 일정이 잡힐 수 있습니다. 공지 날짜, 감사 날짜 및 완료 날짜를 포함한, 실행계획상의 공급업체 감사 정보는 공급업체 상태/일정 내에서 유지됩니다.

안티바이러스 및 안티멀웨어 보호

Medidata는 침입 탐지 시스템(Intrusion Detection System, IDS) 및 방화벽 외에도 다양한 스캐닝 도구를 사용하여 데이터 센터 네트워크를 통과하기 전에 모든 데이터를 더욱 안전하게 처리합니다. 이러한 스캐닝 도구는 악성 소프트웨어 등이 방어를 통과하여 시스템에 액세스를 시도할 경우 이를 알려줍니다. Medidata 네트워크 보안은 "1온스의 예방이 1파운드의 치료보다 낫다"는 옛 속담을 실천하고 있습니다. 이 경우, 멀웨어 스캔이 바로 예방입니다. 엔드포인트 보안은 안티 멀웨어, 엔드포인트 탐지 및 대응, 서버 방화벽, 로그 검사, 침입 탐지 및 방지 모듈을 포함하여, 모든 생산 및 검증 시스템에 설치되어 있습니다.

데이터 암호화

PHI 및 PII를 포함한 모든 데이터는 최신 고급 암호화 표준 알고리즘(AES-256)을 사용하여 암호화된 형태로 저장 및 전송되며, 정기적으로 복구 가능성에 대해 테스트됩니다.

전송 중인 데이터 암호화

이 시스템은 전송 계층 보안 TLS v.1.2를 사용하여 전송 중인 데이터에 대한 암호화를 수행합니다. TLS v.1.2는 클라이언트 컴퓨터가 서버와 공개적으로 액세스할 수 있는 연결을 설정하도록 하지만, 클라이언트와 서버만이 암호를 해독할 수 있거나, 전송되는 정보를 해석 가능하고 사용 가능한 형태로 볼 수 있을 것입니다. TLS 1.3은 구현의 기술적 주류로 채택되고 있습니다.

저장 중 암호화

암호화는 저장 장치 수준에서 활성화되며 하드웨어를 통해 영향을 받습니다. Rave EDC 데이터 저장소의 경우, 퓨어스토리지(PureStorage) 저장소 영역 네트워크는 독점적인 키 관리 시스템을 사용해 256비트 AES 키를 사용합니다. 당사의 멀티테넌트 시스템의 경, 당사는 AES-256도 사용하지만 아마존(Amazon)의 KMS 제품을 사용합니다.

시스템 강화 표준

Medidata는 모든 MCC 구성요소 및 기타 강화 기법에 대한 CIS 벤치마크 경화 지침을 이행합니다.

원격 연결

기본적으로, Medidata는 포트 443의 인바운드 트래픽만 허용합니다. 방화벽과 IDP는 소스 및 대상 포트를 차단하고 트래픽 안전을 보장합니다. 24시간 연중무휴 글로벌 네트워크 운영 센터("GNOC")를 운영하여 누군가가 항상 환경을 모니터링할 수 있도록 지원하고 있습니다. 이외에도, Medidata는 제3자 관리형 보안 서비스 제공자(Managed Security Service Provider, MSSP)를 고용하여 보안 환경을 연중무휴 24시간 보장하며, 서비스 수준 협약(Service Level Agreement, SLA)에 따라 십오(15) 분 단위로 환경 보호를 위한 조치를 취할 수 있는 권한을 부여받았습니다.

개인정보 프로그램

Medidata 개인정보 사무소(“MPO”)는 고객을 대신하여 개인 데이터를 처리하는 Medidata의 역할에 따라 글로벌 개인정보 프로그램 내에서 개인정보 원칙을 구현합니다. Medidata의 고객은 계약된 서비스를 위해 MCC 내에서 제출 및 처리되는 개인 데이터와 관련하여 “데이터 관리자”의 역할을 합니다. 데이터 관리자(또는 관련 법률에 정의된 유사한 주체)는 개인 데이터 처리의 수단과 목적을 결정하는 주체를 말합니다. 즉, Medidata의 고객은 자체 데이터 관리자 역할을 수행하며 임상시험을 위해 MCC를 활용할 때. 어떤 개인 데이터를 수집, 제출, 처리, 공개, 보유, 및/또는 파기할지, 그리고 이러한 활동이 어떤 목적으로 이루어지는지 결정합니다. Medidata의 역할은 “데이터 처리자”의 역할로, 데이터 관리자의 지시를 수행하여 결정된 처리 수단 및 목적을 구현합니다.

데이터 처리자로서 Medidata는 주로 효과적인 데이터 보안 조치를 구현하고 위의 책임 영역과 관련하여 고객의 지시를 따를 책임이 있습니다.

사용자 주체에 대한 개인정보 약속은 고객 계약서/합의서에 문서화되어 전달됩니다. 이러한 개인정보 약속에는 다음이 포함되나, 이에 국한되지 않습니다:

- 관련 계약, 법률, 및 규정에 따라, 시스템 하드웨어 및 민감한 데이터의 적절한 처리와 안전한 유지관리, 폐기 및 파기를 위한, 데이터 보유 및 폐기 정책과 절차.
- MPO는 관련 법률 및 모범 관행에 따라, 고객의 개인 데이터 수집, 액세스, 사용, 저장, 공개 및 폐기를 규제하기 위해, 글로벌 개인정보 프로그램을 유지관리합니다.
- 사용자 주체는 MCC에 로그인할 때 표시되는 ‘이용 약관’의 일부로 개인 데이터와 관련된 Medidata 관행에 대한 정보를 받습니다.
- Medidata는 MCC의 각 제품 릴리스에 대해 “개인정보 중심 설계” 평가를 수행하여 개인 데이터 처리에 대한 영향/중요한 변경사항을 평가합니다.
- Medidata는 고객 개인 데이터의 적절한 액세스 및 사용을 검증하기 위해 고객 데이터 거버넌스 프로그램을 유지관리합니다.
- Medidata는 고객 요청 시 고객 개인 데이터를 반환하거나 삭제합니다(해당 규제/법적 요건에 따라).
- MPO는 고객 개인 데이터의 무단 공개를 식별하고 평가하기 위한 개인정보 사고 대응 프로그램을 유지관리합니다.

개인정보 중심 설계

Medidata는 MCC 전반에 걸쳐 개인 식별 정보의 출처와 위치를 문서화하는 애플리케이션 및 데이터 인벤토리를 공식적으로 문서화했습니다. 애플리케이션 및 데이터 인벤토리는 개인정보 중심 설계 프로세스의 일환으로 각 제품 팀에서 준비합니다. 수집되는 데이터의 종류, 해당 비즈니스 프로세스 내의 관련 개인정보 리스크, 이 프로세스를 통해 식별된 개인정보 리스크를 완화하기 위해 마련된 제어를 명시하는 표준 템플릿이, 각 비즈니스 프로세스 영역별로 문서화되고 유지관리됩니다.

개인정보 중심 설계 프로세스의 일환으로, 제품 소유자는 참여자의 개인정보를 액세스, 사용 및/또는 저장하는 기존 프로세스를 새로 만들거나 변경하는 프로젝트를 평가하여, 개인정보 및 관련 제어에 미치는 영향을 평가합니다. 이러한 변경사항이 확인되면, MPO는 MCC에서 개인 식별 정보를 처리하는 방법의 변경과 관련된 리스크를 평가합니다. 개인정보 중심 설계 프로세스의 일부로 식별된 제어 격차를 문서화하고 격차를 해결하기 위한 시정 조치 계획을 개발 및 실행합니다.

설계에 의한 보안

보안 코딩 표준

Medidata는 OWASP를 기반으로 SDLC 프로세스에 안전한 애플리케이션 개발을 통합합니다. 공식 코딩 표준 및 코딩 가이드라인은 소스 코드 저장소에 저장되어 있으므로, Medidata는 이를 버전 관리하에 보유하고 있습니다.

소프트웨어 개발 수명 주기

MCC는 임상 개발 프로세스 전반의 활동을 관리하도록 설계된 단대단 기술 및 데이터 분석 솔루션을 제공합니다. SaaS 환경으로서 Medidata 플랫폼은 고객의 요구사항에 따라 규모 가변적이며 확장 가능합니다. Medidata는 애자일 개발 원칙에 따라 문서화된 SDLC 프로세스를 준수하여, 프로세스 전반에 걸쳐 품질을 구축함으로써 이를 달성합니다. Medidata는 적격한 인프라에 상주하고, 고객 요구사항을 충족하며, 의도한 대로 기능하고, 해당 GCP, 데이터 보호/데이터 개인정보, 및 전자 기록/전자 서명(Electronic Records/Electronic Signatures, “ERES”) 규정 및 지침 준수를 지원하는 소프트웨어를 생산합니다. SDLC 요건 및 프로세스는 소프트웨어 개발 및 릴리스 절차서에 문서화되어 있습니다. IT 인프라 적격성평가 요건 및 프로세스는 호스팅 환경 아키텍처 관리 문서에 문서화되어 있습니다.

SDLC 활동은 R&D 부서에서 수행합니다. R&D 내에는 직능별 부서가 존재하며, 각 부서는 Medidata 소프트웨어의 설계, 개발, 테스트, 검증, 배포, 및 운영 지원에 대한 관리 책임과 권한을 가지고 있습니다. 소프트웨어 릴리스 유형에는 알파 릴리스, 베타 릴리스, 기능 릴리스, 표준 소프트웨어 릴리스, 및 긴급 소프트웨어 릴리스가 포함됩니다.

취약점 식별 및 관리

Medidata 취약점 평가는 정보 시스템의 잠재적인 보안 취약점을 체계적으로 검토하는 것입니다. 시스템이 알려진 취약점에 취약한지 평가하고, 해당 취약점에 심각도 수준을 할당하며, 필요한 경우 언제든지 교정 또는 완화를 권장합니다.

애플리케이션 보안 취약점 평가

고객을 위해 Medidata가 생산하는 소프트웨어의 보안 취약점 평가를 수행할 때 Medidata의 주요 목표는 권한이 없는 사용자가 획득할 수 없어야 하는 시스템 및 지정된 데이터 액세스 권한을 획득하는 데 이용될 수 있는 시스템, 네트워크 및 애플리케이션 보안 제어의 취약점을 파악하는 것입니다. 평가에는 동적 애플리케이션 보안 테스트(Dynamic Application Security Testing, DAST) 및 정적 애플리케이션 보안 테스트(Static Application Security Testing, SAST) 코드 분석 보안 스캔이 포함되어야 합니다. 테스트의 정의된 매개변수 내에서 작업하면서, Medidata는 위에 명시된 목표를 달성하기 위해, 식별된 모든 시스템, 네트워크 및 애플리케이션 취약성을 식별하고 활용하려고 시도할 것입니다.

스텔스 보안 평가가 아니므로, 공격을 위장하기 위한 어떠한 시도도 하지 않을 것입니다. 실제 공격은 시스템 관리자에게는 분명하지 않을 수 있다는 점에 유의해야 합니다. 테스트 프로세스는 일반적인 취약점 평가에 사용되는 스캐너 및 체크리스트 방법의 일반적인 결과를 제한하기 위해 수동으로 진행될 수 있습니다. 또는, 애플리케이션 매핑 및 잠재적 취약점 식별을 위해 자동화된 도구를 사용할 수도 있습니다. 이러한 방식으로 테스터는 애플리케이션에 대한 표적화된 로직 기반 테스트에 집중할 수 있습니다.

네트워크 보안 취약점 평가(모의 해킹)

Medidata의 네트워크 취약점 평가에는 Medidata 네트워크 외부의 테스트 위치에서 도달할 수 있는 서버, 스위치, 라우터, 및 워크스테이션과 같은 리소스가 포함됩니다. Medidata는 최고 정보 보안 책임자(CISO)가 승인한 신중하게 스크립팅된 테스트 방법론을 사용하여 네트워크 및 구성요소에 대한 테스트를 수행할 것입니다. 참여 규칙에는 수행되는 모든 테스트에 Medidata가 소유 및/또는 운영하지 않는 네트워크 구성요소의 상호 연결 테스트가 포함되지 않는다고 명시되어 있습니다.

이외에도, 테스트에는 시스템에 의도적으로 서비스 거부(Denial of Service, DoS)를 발생시키거나 마주하여 이용 가능한 대상 시스템을 의도적으로 손상시키는 활동은 포함되지 않습니다. 외부 취약점 평가는 물리적 Medidata 위치/네트워크 외부의 위치(들)로부터 수행될 것입니다.

Medidata는 주기적인 취약점 평가 및 모의 해킹을 포함하여, 환경 및 관련 제어에 대한 여러 독립적인 평가를 수행합니다. 이러한 테스트는 전체 환경에 대해, 각각 매주 및 분기별로 실행됩니다. 정보 보안 부서에서 “심각” 또는 “높음”으로 평가한 모든 보안 문제는, 정보 보안 책임자가 서면으로 승인하지 않는 한, 발견일로부터 삼십(30) 일 이내에 교정되어야 합니다. 정보 보안 책임자가
서면으로 승인하지 않는 한, 정보 보안 부서에서 “중간”으로 평가한 모든 보안 문제는, 발견일로부터 달력일 기준 180일 이내에 교정되어야 합니다.

독립적인 테스트 및 검토

보안은 객관적인 관찰자가 명시하는 만큼만 우수합니다. 따라서, 고객 및 규제기관의 평가 외에도, 여러 독립 주체를 정기적으로 교체하여 이용함으로써, 안일함을 방지하고 고객과 환자의 지적 재산이 적절히 보호될 수 있도록, 객관성, 최첨단 기법 및 새로운 기술을 도입하기 위해 노력하고 있습니다.

SOC2는 미국 공인회계사협회(American Institute of CPAs, AICPA)에서 개발한 서비스 조직을 위한 자발적 규정 준수 표준으로, 조직이 고객 데이터를 어떻게 관리해야 하는지 명시하고 있습니다. 이 표준은 보안, 가용성, 처리 무결성, 기밀성, 개인정보와 같은 신뢰 서비스 기준을 기반으로 합니다. SOC2 보고서는 각 조직의 고유한 요구사항에 맞게 조정됩니다. 특정 비즈니스 관행에 따라 각 조직은 하나 이상의 신뢰 원칙을 따르는 제어를 설계할 수 있습니다. 이러한 보고서는 조직과 조직의 고객, 규제기관, 비즈니스 파트너, 및 공급업체에게 조직이 데이터를 관리하는 방식에 대한 중요한 정보를 제공합니다.

2가지 유형의 SOC2 보고서가 있습니다: 유형 1은 조직의 시스템 및 시스템 설계가 관련 신뢰 원칙을 준수하는지 여부를 기술합니다. 유형 2는 이러한 시스템의 운영상의 효율성을 상세히 기술합니다.

Medidata는 TSP 섹션 100, 및 2017 보안, 가용성, 처리 무결성, 기밀성, 및 개인정보에 대한 신뢰 서비스 기준(AICPA, 신뢰 서비스 기준)에 명시된, 보안 및 개인정보 관련 보안(“해당 신뢰 서비스 기준”)에 대한 Medidata의 노력을 입증하기 위해, 그리고 개발 및 배포, 품질 보증, 전자 기록 및 서명과 관련한 Medidata Solutions, Inc.에서 정한 추가 기준에 대한 Medidata의 노력을 입증하기 위해, SOC2+ 유형 2를 유지합니다.

SOC 평가는 단계별 12개월 모집단 시간 단위로 6개월마다 실시됩니다. Medidata는 또한 Medidata 플랫폼 임상시험 관리 시스템(Clinical Trial Management System, CTMS) 사이트 결제 서비스에 대해 SOC-I 유형 2를 유지합니다.

ISO/IEC 27001

ISO 27001은 ISO 27002 모범 관행 지침에 따라 보안 관리 모범 관행 및 포괄적인 보안 제어를 명시하는 보안 관리 표준입니다. 이는 널리 인정받는 국제 보안 표준으로, Medidata 고객들이 큰 관심을 보이고 있습니다.

표준 인증을 받으려면 다음이 요구됩니다:

- 회사의 위협 및 취약점의 영향을 고려하여 정보 보안 리스크를 체계적으로 평가합니다.
- 회사 및 아키텍처 보안 리스크를 해결하기 위한 포괄적인 정보 보안 제어 및 기타 형태의 리스크 관리 제품군을 설계하고 구현합니다.
- 정보 보안 제어가 지속적으로 정보 보안 요구사항을 충족하도록 포괄적인 관리 프로세스를 채택합니다.

이 표준에 따른 인증의 핵심은 엄격한 보안 프로그램을 효과적으로 관리하는 것입니다. 이 표준에 따라 요구되는 정보 보안 관리 시스템(Information Security Management System, ISMS)은 전체적이고 포괄적인 방식으로 보안을 지속적으로 관리하는 방법을 정의합니다. ISO/IEC 27001 인증은 특히 Medidata ISMS에 중점을 두고 있으며, 내부 프로세스가 ISO 표준을 어떻게 따르는지를 측정합니다. 인증은 제3자 공인 독립 감사자가 당사의 프로세스 및 제어에 대한 평가를 수행하여, 당사가 포괄적인 ISO/IEC 27001 인증 표준에 따라 운영하고 있음을 확인했음을 의미합니다.

ISO/IEC 27701

ISO/IEC 27701 인증은 ISO/IEC 27001과 함께 사용되어 개인정보 정보 관리 시스템(Privacy Information Management System, PIMS)의 수립, 구현, 유지관리 및 지속적인 개선을 위한 요건을 다룹니다.

ISO/IEC 27017

ISO/IEC 27701은 클라우드 서비스를 위한 정보 보안 실행 규범입니다. 이는 ISO/IEC 27001 및 ISO/IEC 27002의 확장 버전으로, 클라우드 서비스 제공자와 클라우드 서비스 고객을 위한 추가적인 보안 제어 기능을 제공합니다.

ISO/IEC 27018

ISO/IEC 27018은 클라우드 컴퓨팅 환경의 개인정보 정보 맥락에서 보안 관리 모범 관행과 포괄적인 보안 제어를 명시하는 보안 관리 표준입니다. 이 표준은 개인정보 관련 정보의 효과적인 관리를 유지하기 위해 ISO/IEC 27001 및 기타 보안 프레임워크를 보완합니다.

ISO/IEC 27001, ISO/IEC 27017, 27018과 마찬가지로, 인증은 제3자 공인 독립 감사자가 당사의 프로세스 및 제어에 대한 평가를 수행하여, 당사가 포괄적인 ISO 27018 인증 표준에 따라 운영하고 있음을 확인했음을 의미합니다.

FISMA 중간

Medidata는 미국 정부 기관 고객이 미국 연방정보보안관리법(Federal Information Security Management Act, FISMA)을 준수하고 이를 유지할 수 있도록 합니다. FISMA는 연방 기관이 미국 국립표준기술연구소(National Institute of Standards and Technology, NIST) 특별 간행물 SP 800-53, 개정 5에 따라, 데이터 및 인프라를 위한 정보 보안 시스템을 개발, 문서화. 및 구현하도록 규정하고 있습니다. FISMA는 Medidata가 광범위한 보안 구성 및 제어를 구현하고 운영하도록 요구합니다. 여기에는 확립된 프로세스 및 제어에 대한 제3자 감사를 문서화하는 것뿐만 아니라, 물리적 및 가상 인프라를 보호하는 데 사용되는 관리, 운영 및 기술 프로세스가 포함됩니다. Medidata는 매년 서비스형 소프트웨어에 대한 FISMA 규정 준수 유지에 대해 평가받고 있으며, 다수의 미국 정부 기관으로부터 운영 권한(Authority to Operate, ATO)을 획득했습니다.

EU-US 데이터 개인정보 프레임워크(DPF) 및 관련 프레임워크

EU-US 데이터 개인정보 프레임워크와 영국 의 EU-US DPF 확장 및 스위스-US DPF와 같은 관련 프레임워크는, 유럽연합, 영국 및 스위스에서 미국으로 개인 데이터 전송을 위한 신뢰할 수 있는 메커니즘을 Medidata에 제공하는 동시에, EU, 영국 및 스위스 법과 일치하는 데이터 보호를 보장합니다. EU-US DPF 및 관련 프레임워크에 참여하는 조직은 개인 데이터를 받을 수 있습니다: (1) EU에서 EU-US DPF에 대한 유럽연합 집행위원회의 적정성 결정 발효일인 2023년 7월 10일부터, (2) 영국에서 영국 확장을 시행하는 적정성 규정의 발효일인 2023년 10월 12일부터, 그리고 (3) 스위스에서 스위스가 스위스-US DPF에 대한 적정성을 인정하는 발효일부터. EU-US DPF 및 관련 프레임워크는 전 세계에서 EU, 영국 및 스위스 시민의 개인 데이터를 보호해야 한다는 강력한 의무를 미국 회사에 부과합니다.

실제로는 어떤 의미입니까?

Medidata Solutions 의 경우

- EU-US DPF 원칙 준수(고지, 선택, 전달 책임, 보안, 데이터 무결성 및 목적 제한, 액세스, 상환청구, 집행 및 책임).
- EU-US DPF에 따른 요건을 충족한다는 것을 매년 자체 인증.

유럽, 영국 및 스위스의 Medidata Solutions 고객의 경우

- 개인 데이터의 미국 이전에 대한 투명성을 높이고 개인 데이터에 대한 보호 강화.
- EU-US DPF 웹사이트 https://dataprivacyframework.gov를 방문하여 Medidata의 EU-US DPF 본인인증 검증 가능.

FIPS 140-2

미연방 정보처리 표준(FIPS) 간행물 140-2는 민감한 정보를 보호하는 암호 모듈에 대한 보안 요건을 명시하는 미국 정부 보안 표준입니다. 고객에게 FIPS 140-2 요건을 지원하기 위해, Medidata Private Cloud 엔드포인트와 Medidata 내 종단 로드 밸런서는 FIPS 140-2 검증 알고리즘을 사용하여 작동합니다. FIPS-140-2 준수 모드로 작동하려면 연결의 사용자 브라우저 측에서 유사한 기능이 필요합니다. FIPS 140-2 인증 하드웨어는 사용하지 않지만, 당사는 완전히 승인된 FIPS 140-2 소프트웨어와 유사한 제조사 및 모델을 사용합니다.

HIPAA

Medidata가 제공하는 특정 서비스에 따라 요구되는 경우, Medidata는 미국 건강보험의 양도성과 책임에 대한 법률(Health Insurance Portability and Accountability Act, HIPAA)의 적용을 받는 대상 기업 및 해당 비즈니스 관계자가, 안전한 Medidata 환경을 활용하여 보호된 건강 정보를 처리, 유지관리 및 저장할 수 있도록 합니다.

마침말

당사는 Medidata 보안 관행이 최고의 인력, 프로세스 및 기술로 구성된 세계적 수준이라고 생각합니다. 당사는 당사의 책임을 진지하게 받아들이고 매일 당사의 고객 및 그들의 환자의 신뢰를 얻습니다. 당사는 당사가 하는 일이 자랑스러우며 이를 보여드릴 수 있어 기쁩니다.

환자가 기대하는 보호 수준에서 당사의 고객 및 그들의 시험기관이 안심할 수 있도록, 당사는 본 문서 외에도, 취약점 요약, 모의 해킹 결과, 인증, 감사 및 기타 보안 관련 사항을 https://www.medidata.com/en/trust-and-transparency에 게시하고 있습니다.

질문이 있거나 명확한 설명이 필요하시면, 언제든지 Medidata 정보 보안 프레임워크 팀(asksecurity@3ds.com)으로 문의하십시오.

면책조항

본 보안 백서에 포함된 정보는 참고용으로만 제공됩니다.

본 문서에 포함되거나 고객에게 구두로 전달되는 어떠한 내용도 해당 고객과 Medidata 또는 Medidata 자회사 또는 계열사(총칭하여, “Medidata”) 간의 서면 계약 조건을 개정, 수정, 또는 대체하는 것으로 간주되지 않을 것입니다.

Medidata는 본 보안 백서에 기술된 방법이나 제안이 고객의 시스템을 복구하고, 악성 코드와 관련된 문제를 해결하거나, 기타 명시되거나 의도된 결과를 달성할 것이라는 약속 또는 보증을 고객에게 제공하지 않습니다. 고객은 본 보안 백서에 기술된 지침을 활용하거나 활용하지 않을 경우의 모든 리스크를 전적으로 부담합니다.