솔루션 개요

THALES

CYBERSECURITY

미국 의료정보 보호법 (HIPAA) 데이터 보안 규정 준수

Thales 솔루션이 HIPAA 준수를 지원하는 방법

cpl.thalesgroup.com

THALES

CYBERSECURITY

미국 의료 정보 보호법 (HIPAA)이란 무엇인가요?

미국 의료정보 보호법(HIPAA)은 환자의 동의나 인지 없이 민감한 환자 건강 정보가 공개되는 것을 방지하기 위한 전국적 기준을 마련한 미국 연방 법률입니다. 미국 보건복지부(HHS) HIPAA는 요구사항을 이행하기 위해 HIPAA 개인정보 보호 규칙을 발표했습니다. HIPAA 보안 규칙은 개인정보 보호 규칙이 적용하는 정보의 일부를 보호합니다.

HIPAA 법규는 규정 준수에 필요한 세 가지 유형의 보안 보호 조치를 규정합니다:

- **관리적 보호 조치**는 주로 PHI의 무결성에 대한 잠재적 취약성과 위험을 파악하기 위한 지속적인 위험 평가 수행 요건과 관련됩니다.
- **물리적 보호 조치**는 PHI에 대한 무단 접근을 방지하고 화재 및 기타 환경적 위험으로부터 데이터를 보호하기 위해 시행해야 할 조치에 중점을 둡니다.
- **기술적 보호 조치**는 PHI가 전자 네트워크를 통해 전달될 때 데이터 보안을 보장하기 위해 마련해야 할 통제 장치와 관련됩니다.

어떤 기업이 HIPAA의 적용을 받나요?

HIPAA 규정은 적용 대상 기관(Covered Entities)과 비즈니스 파트너(Business Associates)에게 적용됩니다:

- 적용 대상 기관은 건강 계획, 건강 보험 기관, 병원, 클리닉, 약국, 의사, 치과의사 등 보호된 개인 건강 정보(PHI)를 생성, 수신, 유지, 전송 또는 접근하는 모든 의료 서비스 제공자를 포함합니다.
- 비즈니스 파트너는 적용 대상 기관을 대신하여 전자 PHI를 생성, 수신, 유지, 전송 또는 접근할 수 있는 제3자 서비스 제공업체를 포함합니다. IT 계약업체 또는 클라우드 스토리지 업체 등이 이에 해당합니다.

HIPAA는 언제 발효되었나요?

HIPAA는 1996년 미국 의회에서 제정되었습니다. 이후 2009년 경제적 및 임상적 건강을 위한 보건 정보 기술법(HITECH) 통과 등을 통해 여러 차례 업데이트되었으며, 이를 통해 위반에 대한 새로운 처벌 구조가 추가되고 비즈니스 파트너가 보안 규칙 미준수로 인한 데이터 침해에 대해 직접적인 책임을 지게 되었습니다.

HIPAA 미준수에 따른 처벌은 무엇인가요?

HIPAA 미준수에 대한 처벌은 과실 수준에 따라 다르며, 개별 위반 건당 100달러에서 50,000달러까지 부과될 수 있고, 연간 최대 처벌 금액은 190만 달러입니다. 위반 시 책임자에게 1년에서 10년의 징역형이 처해질 수도 있습니다.

Thales는 HIPAA 준수를 어떻게 도울 수 있나요?

Thales의 솔루션은 보안을 자동화하고 규정 준수를 간소화하여 보안 및 컴플라이언스 팀의 부담을 줄여줌으로써 조직이 HIPAA를 준수하도록 도울 수 있습니다. 당사는 법의 네 가지 섹션에 따른 PHI 보호 필수 요구 사항을 해결함으로써 조직의 HIPAA 준수를 지원합니다:

164.306 보안 표준: 일반 규칙

적용 대상 기관은 기관 또는 비즈니스 파트너가 생성, 수신, 유지 또는 전송하는 모든 전자 보호 건강 정보의 기밀성, 무결성 및 가용성을 보장해야 합니다.

Thales 지원 방법:

- **하이브리드 IT 전반에서 민감한 데이터를 식별, 분류, 보호 및 모니터링합니다.**

HIPAA 요구 사항	Thales 역량	Thales 솔루션
하이브리드 IT 전반에서 민감한 데이터를 식별, 분류, 보호 및 모니터링합니다.	하이브리드 IT 전반에서 민감한 데이터를 식별, 분류, 보호 및 모니터링하여 데이터가 항상 안전하고 규정을 준수하도록 보장합니다.	CipherTrust Platform Data Security Fabric

HIPAA § 164.308 행정적 보호 조치

적용 대상 기관은 PHI에 대한 위험을 정확하고 철저하게 평가해야 하며, 비즈니스 파트너는 PHI를 적절하게 보호해야 합니다.

Thales 지원 방법:

- 위험 분석 수행
- 악성 소프트웨어로부터 보호
- 제 3자(비즈니스 파트너) 위험 감소

HIPAA 요구 사항	Thales 역량	Thales 솔루션
1. A "전자적으로 보호된 건강 정보의 기밀성 및 무결성에 대한 위험 평가 수행…	• 하이브리드 IT 환경 전반에서 위험에 노출된 정형·비정형 민감 데이터를 식별합니다. • 데이터 자산의 위험 점수를 산정하여 잠재적 위험을 평가합니다. • 현재 규정 준수 상태를 파악하고 미비점을 문서화합니다. • 모든 공개, 비공개 및 섀도우 API의 잠재적 위험을 발견·분류하고 API 위험 평가를 수행합니다.	**애플리케이션 보안** API 보안 **데이터 보안** 데이터 검색 및 분류 데이터 위험 인텔리전트 취약점 관리
5, b: "악성 소프트웨어로부터 보호	• I/O를 모니터링하고 랜섬웨어가 침투하기 전에 의심스러운 활동을 차단합니다. • 악성 소프트웨어와 사용자가 민감한 데이터에 접근하는 것을 방지합니다. • 서명, 행동 및 평판 분석을 사용하여 모든 악성 소프트웨어 삽입 공격을 차단합니다. • 웹 애플리케이션 방화벽으로 사이버 위협을 탐지하고 방어합니다. • DDoS 공격과 악성 봇으로부터 중요 네트워크 자산을 보호합니다.	**애플리케이션 보안** 봇 방어 **데이터 보안** 랜섬웨어 보호 데이터 위험 인텔리전트
8. b. 1 "적용 대상 기관은 비즈니스 파트너가 정보를 적절하게 보호할 경우… 비즈니스 파트너가 전자 PHI를 생성, 수신, 유지 또는 전송하도록 허용할 수 있습니다."	• 클라우드에 호스팅된 데이터를 보호하는 암호화 키에 대해 온프레미스 제어권을 유지함으로써 제3자 위험을 줄입니다. • 클라우드 제공업체 관리자와 귀하의 조직 간의 역할 분립을 시행하고 민감한 데이터에 대한 액세스를 제한합니다. • 이상 징후를 모니터링 및 경고하여 공급망 공격으로 이어질 수 있는 비정상 활동을 탐지하고 방지 합니다. • 명확한 액세스 권한 위임을 통해 공급업체, 파트너 또는 제3자 사용자와의 관계 관리를 지원합니다. • 관계 기반의 세분화된 권한 부여를 사용하여 권한을 최소화합니다. • 제3자 사용자가 MFA를 사용하도록 하여 피싱 공격을 저지합니다.	**데이터 보안** 클라우드 키 관리 투명 암호화 데이터 활동 모니터링 사용자 권한 관리 검색 및 분류 **ID 및 접근 관리** 임직원 접근 관리 제3자 접근 제어 위임 사용자 관리 외부화된 인가

HIPAA § 164.312 기술적 보호 조치

적용 대상 기관은 보호된 정보에 대한 접근 보안, PHI에 접근하는 사람 및 기관의 인증, 정지 상태 및 전송 중인 PHI 암호화를 위한 기술적 보호 조치를 시행해야 합니다.

Thales 지원 방법:

- PHI 접근 관리
- 사용자 및 프로세스 인증
- 정지 상태의 PHI 암호화 및 암호화 키 보호
- 전송 중인 PHI 암호화

HIPAA 요구 사항	Thales 역량	Thales 솔루션
A, 1: "접근 권한이 부여된 사람 또는 소프트웨어 프로그램에만 PHI 접근을 허용합니다."	• 하이브리드 IT 환경 전반에서 위험에 노출된 정형·비정형 민감 데이터를 식별합니다. • 데이터 자산의 위험 점수를 산정하여 잠재적 위험을 평가합니다. • 현재 규정 준수 상태를 파악하고 미비점을 문서화합니다. • 모든 공개, 비공개 및 섀도우 API의 잠재적 위험을 발견·분류하고 API 위험 평가를 수행합니다.	**애플리케이션 보안** API 보안 **데이터 보안** 데이터 검색 및 분류 데이터 위험 인텔리전트 취약점 관리
B: "감사 제어. 전자 PHI를 포함하거나 사용하는 정보 시스템의 활동을 기록하고 검토하는 하드웨어, 소프트웨어 및/또는 절차적 메커니즘을 구현하십시오."	• 하이브리드 IT의 정형 및 비정형 데이터에 대한 데이터 활동 모니터링을 수행합니다. • 모든 시스템에 대한 모든 액세스 이벤트의 감사 추적(Audit trail) 및 보고서를 생성하고 로그를 SIEM으로 스트리밍합니다.	**데이터 보안** 데이터 활동 모니터링 투명암호화
D: "전자 PHI에 대한 접근을 요청하는 사람 또는 기관이 주장하는 당사자임을 인증합니다."	• 가장 광범위한 하드웨어 및 소프트웨어 방식으로 다중 인증(MFA)을 활성화합니다. • 데이터/애플리케이션의 민감도에 따라 적응형 인증 정책을 구축하고 배포합니다. • 피싱 및 중간자 공격으로부터 보호합니다.	**ID 및 접근 관리(IAM)** 다중 인증(MFA) 위험 기반 인증 PKI 및 FIDO 인증기
2, ii: "전자적으로 보호된 건강 정보를 암호화하고 복호화하는 메커니즘을 구현합니다."	• 온프레미스, 클라우드 전반, 빅데이터 또는 컨테이너 환경에서 정지 상태의 데이터를 암호화합니다. • FIPS 140-2 Level 3 환경에서 암호화 키를 보호합니다. • 데이터베이스의 민감한 정보를 가명화합니다. • 기밀 컴퓨팅(Confidential Computing)을 활용하여 사용 중인 데이터를 보호합니다. • 완전한 민감 데이터 활동 가시성을 확보하고 접근자를 추적하며 활동을 감사하고 문서화합니다. • 암호화 민첩성을 유지하기 위한 양자 내성 암호화 전환을 위해 설계된 보안 제품입니다.	**데이터 보안** 투명 암호화 토큰화 키 및 시크릿 관리 하드웨어 보안 모듈(HSM) 기밀 컴퓨팅 데이터 거버넌스 데이터 활동 모니터링

HIPAA 요구 사항	Thales 역량	Thales 솔루션
E. 1: "네트워크를 통해 전송되는 PHI를 보호하기 위한 기술적 보안 조치를 구현합니다."	• 고속 암호화로 전송 중인 데이터를 보호합니다.	**데이터 보안** 고속 암호화

HIPAA § 164.514
개인건강정보의 이용 및 공개에 관한 기타 요건

개인 식별이 불가능한 건강정보는 PHI (개인건강정보)로 간주되지 않습니다.

- **Thales는 다음과 같은 방식으로 조직을 지원합니다:**
  토크나이제이션(Tokenization)을 활용한 개인건강정보의 가명처리 및 비식별화.

HIPAA 요구 사항	Thales 역량	Thales 솔루션
A "보호된 건강 정보의 비식별화. 개인을 식별하지 않는 건강 정보...는 개인 식별 가능한 건강 정보가 아닙니다."	• 민감한 PHI를 노출하지 않고 집계 데이터를 분석하는 능력을 유지하면서 생산 또는 테스트 목적으로 민감한 정보를 가명화하고 마스킹합니다.	**데이터 보안** 토큰화 데이터 마스킹

Thales는 애플리케이션 보안, 데이터 보안, 신원 및 접근 관리 등 사이버 보안 세 가지 핵심 영역에서 포괄적인 솔루션을 제공합니다.

- **애플리케이션 보안:** 클라우드, 온프레미스 또는 하이브리드 모델에서 대규모로 애플리케이션과 API를 보호합니다. 시장을 선도하는 당사의 제품군에는 분산 서비스 거부(DDoS) 및 악성 봇 공격에 대한 웹 애플리케이션 방화벽(WAF) 보호, API 보안, 안전한 콘텐츠 전송 네트워크(CDN), 런타임 애플리케이션 자가 보호(RASP)가 포함됩니다.
- **데이터 보안:** 하이브리드 IT 전반에서 민감한 데이터를 발견하고 분류하며, 암호화, 토큰화 및 키 관리를 사용하여 정지 상태, 이동 중 또는 사용 중 어디서나 자동으로 보호합니다. Thales 솔루션은 또한 정확한 위험 평가를 위해 잠재적 위험을 식별, 평가 및 우선순위를 지정하고, 비정상적인 행동을 식별하며 활동을 모니터링하여 잠재적 위협을 파악하고 규정 준수를 검증합니다.
- 신원 및 접근 관리: 고객, 직원 및 파트너를 위한 애플리케이션과 디지털 서비스에 대한 원활하고 안전하며 신뢰할 수 있는 접근을 제공합니다. 당사의 솔루션은 세분화된 접근 정책과 다중 인증을 통해 역할 및 상황에 따라 내부 및 외부 사용자의 접근을 제한하여 올바른 사용자가 올바른 시간에 올바른 자원에 접근할 수 있도록 지원합니다.

Thales 소개

오늘날의 기업과 정부는 신뢰할 수 있는 디지털 서비스를 제공하기 위해 클라우드, 데이터 및 소프트웨어에 의존합니다. 그렇기 때문에 전 세계에서 가장 유명한 브랜드와 기관들이 클라우드와 데이터 센터부터 기기와 네트워크에 이르기까지 민감한 정보와 소프트웨어가 생성, 저장 또는 접근되는 모든 곳에서 이를 보 호하기 위해 Thales에 의존합니다. 데이터 보안 및 소프트웨어 라이선싱 분야의 글로벌 리더로서, 당사의 솔루션은 기관이 안전하게 클라우드로 이전하고, 자신 있게 규정 준수를 달성하며, 소프트웨어에서 더 많은 가치를 창출하고, 매일 수백만 소비자에게 원활한 디지털 경험을 제공할 수 있도록 합니다.

cpl.thalesgroup.com

문의하기 – 연락처 정보는 cpl.thalesgroup.com/contact-us에서 확인하세요.