



Data Security Compliance with the Health Insurance Portability and Accountability Act (HIPAA)

How Thales solutions help
HIPAA compliance

cpl.thalesgroup.com

THALES
Building a future we can all trust

What is the Health Insurance Portability and Accountability Act (HIPAA)?

The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that created national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule.

HIPAA Rules and Regulations lay out three types of security safeguards required for compliance:

- **Administrative Safeguards** primarily concern the requirement to conduct ongoing risk assessments to identify potential vulnerabilities and risks to the integrity of PHI.
- **Physical Safeguards** concentrate on the measures that should be implemented to prevent unauthorized access to PHI and to protect data from fire and other environmental hazards.
- **Technical Safeguards** relate to the controls that must be put in place to ensure data security when PHI is being communicated on an electronic network.

Which companies are subject to HIPAA?

The HIPAA Rules apply to covered entities and business associates:

- Covered Entities encompass all health care providers creating, receiving, maintaining, transmitting, or accessing protected personal health information (PHI), including health plans, health insurance organizations, hospitals, clinics, pharmacies, physicians, and dentists, among others.

- Business Associates encompass third-party service providers that may create, receive, maintain, transmit, or access ePHI on behalf of covered entities. Examples include IT contractors or cloud storage vendors.

When did HIPAA go into effect?

HIPAA was enacted by the US congress in 1996. The law has been updated several times since, such as in 2009 with the passing of the Health Information Technology for Economic and Clinical Health Act (HITECH), which added a new penalty structure for violations and made Business Associates directly liable for data breaches attributable to non-compliance with the Security Rule.

What are the penalties for HIPAA non-compliance?

The penalties for non-compliance with HIPAA vary based on the perceived level of negligence and can range from \$100 to \$50,000 per individual violation, with a maximum penalty of \$1.9 million per calendar year. Violations can also result in jail time of one to ten years for the individuals responsible.

How can Thales help with HIPAA compliance?

Thales' solutions can help organizations comply with HIPAA by simplifying compliance and automating security, reducing the burden on security and compliance teams. We help organizations comply with HIPAA by addressing essential requirements for safeguarding protected health information (PHI) under four different sections of the law:

164.306 Security standards: General rules

Covered entities must ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmit.

Thales helps organizations by:

- Identifying, classifying, protecting, and monitoring sensitive data across hybrid IT.

HIPAA	Thales Capabilities	Thales Solutions
1. Ensure confidentiality, integrity, and availability of electronic PHI.	Identify, classify, protect, and monitor sensitive data across hybrid IT, ensuring that data is always secure and in compliance.	CipherTrust Platform Data Security Fabric

HIPAA § 164.308 Administrative Safeguards

Covered entities must conduct an accurate and thorough assessment of the risks to PHI and business associates need to appropriately safeguard PHI.

Thales helps organizations by:

- Performing a risk analysis
- Protecting from malicious software
- Reducing third party (business associate) risk

HIPAA	Thales Capabilities	Thales Solutions
<p>1. A “Conduct ... assessment of risks to the confidentiality and integrity of electronic protected health information...”</p>	<ul style="list-style-type: none"> • Identify structured and unstructured sensitive data at risk across Hybrid IT. • Determine risk scores for data assets to assess potential risks. • Identify current state of compliance, documenting gaps. • Discover and classify potential risk for all public, private, and shadow APIs and conduct API risk assessment. 	<p>Application Security API Security</p> <p>Data Security Data Discovery & Classification Data Risk Intelligence Vulnerability Management</p>
<p>5, b: “Protection from malicious software.”</p>	<ul style="list-style-type: none"> • Monitor I/O and block suspicious activity before ransomware can take hold • Prevents malicious software and users from accessing sensitive data. • Use signature, behavioral and reputational analysis to block all malware injection attacks. • Detect and prevent cyber threats with web application firewall. • Safeguard critical network assets from DDoS attacks and Bad Bots. 	<p>Application Security Web Application Firewall DDoS Protection Bot Protection</p> <p>Data Security Ransomware Protection Data Risk Intelligence</p>
<p>8. b. 1 “A covered entity may permit a business associate to create, receive, maintain, or transmit electronic PHI if...business associate will appropriately safeguard the information.”</p>	<ul style="list-style-type: none"> • Reduce third party risk by maintaining on-premises control over encryption keys protecting data hosted by in the cloud. • Enforce separation of roles between cloud provider admins and your organization, restrict access to sensitive data. • Monitor and alert anomalies to detect and prevent unwanted activities from disrupting supply chain activities. • Enable relationship management with suppliers, partners or any third-party user; with clear delegation of access rights. • Minimize privileges by using relationship-based fine-grained authorization. • Enable MFA for third-party users to thwart phishing attacks. 	<p>Data Security Cloud Key Management Transparent Encryption Data Activity Monitoring User Rights Management Discovery and Classification</p> <p>Identity & Access Management Workforce Access Management Third-party Access Control Delegated User Management Externalized Authorization</p>

HIPAA § 164.312 Technical Safeguards

Covered entities must implement technical safeguards to secure access to protected information, authenticate persons and entities accessing PHI, and encrypt PHI at rest and in transit.

Thales helps organizations by:

- Managing access to PHI
- Authenticating users and processes
- Encrypting PHI at rest and protecting encryption keys
- Encrypting PHI in transit

HIPAA	Thales Capabilities	Thales Solutions
A, 1: “Allow access to PHI only to those persons or software programs that have been granted access rights”	<ul style="list-style-type: none"> • Limit access to systems and data based on roles and context with policies. • Apply contextual security measures based on risk scoring. • Leverage smart cards for implementing physical access to sensitive facilities. • Provide customers secure access to their information in company’s systems. • Limit access to systems and data based on roles and context with policies. 	<p>Identity & Access Management Workforce Access Management Customer Identity & Access Management</p> <p>Data Security Transparent Encryption Data Activity Monitoring</p>
B: “Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.”	<ul style="list-style-type: none"> • Data activity monitoring for structured and unstructured data on Hybrid IT. • Produce audit trail and reports of all access events to all systems, stream logs to SIEM. 	<p>Data Security Data Activity Monitoring Transparent Encryption</p>
D: “Authenticate that a person or entity seeking access to electronic PHI is the one claimed.”	<ul style="list-style-type: none"> • Enable multi-factor authentication (MFA) with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies based on the sensitivity of the data/application. • Protect against phishing and man-in-the-middle attacks. 	<p>Identity & Access Management Multi-Factor Authentication Risk-Based Authentication PKI and FIDO Authenticators</p>
2, ii: “Implement a mechanism to encrypt and decrypt electronic protected health information.”	<ul style="list-style-type: none"> • Encrypt data at rest on-premises, across clouds, and in big data or container environments. • Protect cryptographic keys in a FIPS 140-2 Level 3 environment. • Pseudonymize sensitive information in databases. • Protect data in use by leveraging confidential computing. • Gain full sensitive data activity visibility, track who has access, audit what they are doing and document. • Security products designed for post-quantum upgrade to maintain crypto-agility. 	<p>Data Security Transparent Encryption Tokenization Key & Secrets Management Hardware Security Modules Confidential Computing Data Governance Data Activity Monitoring</p>

HIPAA	Thales Capabilities	Thales Solutions
E. 1: “Implement technical security measures to protect PHI being transmitted over...a network.”	<ul style="list-style-type: none"> Protect data-in-motion with high speed encryption. 	Data Security High Speed Encryption

HIPAA § 164.514
Other requirements relating to uses and disclosures of protected health information

Health information may not be considered PHI if it is not individually identifiable health information.

Thales helps organizations by:

- Pseudonymizing and de-identifying personal health information using tokenization.

HIPAA	Thales Capabilities	Thales Solutions
A “De-identification of protected health information. Health information that does not identify an individual...is not individually identifiable health information.”	<ul style="list-style-type: none"> Pseudonymize and mask sensitive information for production or tests while maintaining ability to analyse aggregate data without exposing sensitive PHI. 	Data Security Tokenization Data Masking

Thales provides comprehensive cyber security solutions in three key areas of cybersecurity: Application Security, Data Security, and Identity & Access Management.

- Application Security:** Protect applications and APIs at scale in the cloud, on-premises, or in a hybrid model. Our market leading product suite includes Web Application Firewall (WAF) protection against Distributed Denial of Service (DDoS) and malicious BOT attacks, security for APIs, a secure Content Delivery Network (CDN), and Runtime Application Self-Protection (RASP).
- Data Security:** Discover and classify sensitive data across hybrid IT and automatically protect it anywhere, whether at rest, in motion, or in use, using encryption, tokenization, and key management. Thales solutions also identify, evaluate, and prioritize potential risks for accurate risk assessment. They also identify anomalous behaviour and monitor activity to identify potential threats and verify compliance, allowing organizations to prioritize where to allocate their efforts.

- Identity & Access Management:** Provide seamless, secure, and trusted access to applications and digital services for customers, employees, and partners. Our solutions limit the access of internal and external users based on their roles and context with granular access policies and multi-factor authentication that help ensure that the right user is granted access to the right resource at the right time.

About Thales

Today’s businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Disclaimer: The information contained herein is believed to be accurate on the date of publishing. Thales provides this material for your information only. Its content is not legal advice nor does it amount to a certification or guarantee of compliance in respect of any applicable law. Third parties shall be solely responsible for their own interpretation of any applicable law. The information should not be construed as a commitment to deliver any specific upgrade, feature or functionality. You should not rely on the anticipated timelines or potential upgrades, features or functionality described in the presentation when making a decision to purchase products from Thales. Thales does not accept any liability howsoever arising from any use of this material.