cpl.thalesgroup.com

THALES
Building a future we can all trust

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

How Thales solutions help with HIPAA Compliance

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 helps organizations comply with HIPAA by addressing essential requirements for safeguarding protected health information (PHI) under three different sections of the law.

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:

- Discovering and classifying sensitive data and performing risk analysis
- Reducing third party (business associate) risk

HIPAA	Requirement	Thales Solutions
1. A	"Conduct **...assessment of risks to the confidentiality and integrity of electronic protected health information...**"	**CipherTrust Data Discovery and Classification** identifies structured and unstructured sensitive data on-premises and in the cloud. Built-in templates enable rapid identification of regulated data, highlight security risks, and help uncover compliance gaps.
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."**	**CipherTrust Cloud Key Manager** can reduce third party risks by maintaining on-premises under the full control of the healthcare institution the keys that protect sensitive data hosted by third party cloud providers. This increases operational efficiency through harmonization and automation. **CipherTrust Transparent Encryption** provides complete separation of administrative roles, so only authorized users and processes can view unencrypted data. Sensitive data stored in a third-party cloud will not be accessible in cleartext to unauthorized users. These could include third party cloud provider employees, such as support engineers, DB admins, or potentially malicious processes. In addition, **Thales Portfolio of Data Security** solutions offer the most comprehensive range of data protection, such as **Thales Data Protection on Demand (DPoD)** that provides built in high availability and backup to its cloud-based **Luna Cloud HSM** and **CipherTrust Key Management** services, to the **HSE** network encryption appliances that provides options to zeroize.

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

How can Thales help with HIPAA compliance?

HIPAA	Requirement	Thales Solutions
A. 1	**"Allow access to PHI only to those persons or software programs that have been granted access rights"**	**Thales OneWelcome** identity & access management products and solutions limit the access of internal and external users based on their roles and context. Backed by strong authentication (MFA), granular access policies and fine-grained authorization policies help ensuring that the right user is granted access to the right resource at the right time; whereby minimizing the risk of unauthorized access. **Thales OneWelcome Consent & Preference Management** module enables organizations to gather consent of end consumers such that healthcare institutions may have clear visibility of consented data, thereby allowing them to manage access to data that they are allowed to utilize. **CipherTrust Transparent Encryption** encrypts sensitive data and enforces granular privileged-user-access management policies that can be applied by user, process, file type, time of day, and other parameters. The solution provides complete separation of roles where only authorized users and processes can view unencrypted data.
D	**"Authenticate that a person or entity seeking access to electronic PHI is the one claimed."**	**SafeNet Trusted Access** provides commercial, off-the-shelf multi-factor authentication with the broadest range of hardware and software authentication methods and form factors. This allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally-managed policies— all managed from one authentication back end delivered in the cloud or on-premises. **SafeNet IDPrime** smart cards can be leveraged for implementing physical access to sensitive facilities. These smart cards can also augment Passwordless authentication initiatives relying on PKI and FIDO technology.
2, ii	**"Implement a mechanism to encrypt and decrypt electronic protected health information."**	**CipherTrust Data Security Platform** provides multiple capabilities for protecting data at rest in files, volumes, and databases. Among them: • **CipherTrust Transparent Encryption** delivers data-at-rest encryption with centralized key management and privileged user access control. This protects data wherever it resides, on-premises, across multiple clouds, and within big data and container environments. • **CipherTrust Enterprise Key Management** streamlines and strengthens key management in cloud and enterprise environments over a diverse set of use cases. Leveraging FIPS 140-2-compliant virtual or hardware appliances, our key management tools and solutions deliver high security to sensitive environments and centralize key management for home-grown encryption, as well as third-party applications. **Thales Luna Hardware Security Modules (HSMs)** protect cryptographic keys and provide a FIPS 140-2 Level 3 hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, and more. Luna HSMs are available on-premises, in the cloud as-a-service, and across hybrid environments. • Generates and protects root and certificate authority (CA) keys, providing support for PKIs across a variety of use cases • Signs application code to ensure software remains secure, unaltered, and authentic • Creates digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other network deployments

How can Thales help with HIPAA compliance?

HIPAA	Requirement	Thales Solutions
E. 1	**"Implement technical security measures to protect PHI being transmitted over... a network."**	**Thales High Speed Encryptors (HSEs)** provide network-independent data-in-motion encryption (layers 2, 3, and 4) ensuring data is secure as it moves from site-to-site, or from on-premises to the cloud and back. Our network encryption solutions allow customers to better protect data, video, voice, and metadata from eavesdropping, surveillance, and overt and covert interception — without performance compromise. Thales HSEs are available as both physical and virtual appliances, supporting a wide spectrum of network speeds from 10 Mbps to 100 Gbps. Rigorously tested and certified to exacting standards such as FIPS 140-2 L3 and Common Criteria, Thales HSE network encryption solutions have been vetted by such organizations as the USA Department of Defense Information Network (DoDIN) and NATO.

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	Requirement	Thales Solutions
A	**"De-identification of protected health information.** Health information that does not identify an individual...is not individually identifiable health information."	**CipherTrust Tokenization** permits the pseudonymization (and consequently, de-identification) of sensitive information in databases while maintaining the ability to analyze aggregate data without exposing sensitive data during the analysis or in reports.

About Thales

Thales is a global leader in data security, trusted by governments and the most recognized companies around the world to help them protect their most sensitive data. The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.