White Paper

THALES

CYBERSECURITY

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

How Thales can help your organization comply with the latest HIPAA updates

cpl.thalesgroup.com

THALES

CYBERSECURITY

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) is a U.S. federal law enacted in 1996 to protect the privacy and security of individuals' health information. It establishes national standards for how healthcare data can be used, stored, and shared by organizations that handle medical information. HIPAA was originally designed to improve the portability of health insurance when people change jobs, but it has become most widely known for its role in safeguarding sensitive health data and setting requirements for the protection of electronic healthcare information.

Electronic Protected Health Information (ePHI)

A central concept within HIPAA is Protected Health Information (PHI). PHI includes any information that can identify an individual and relates to their health status, healthcare services, or payment for healthcare. This can include medical records, lab results, billing information, insurance details, and appointment histories. When this information is created, stored, or transmitted electronically, it is referred to as electronic Protected Health Information (ePHI). HIPAA requires organizations to implement safeguards to ensure that this data is kept confidential, secure, and available only to authorized individuals.

HIPAA rules and safeguards

HIPAA is implemented through several regulatory rules that define how healthcare data must be protected.

- **The Privacy Rule** establishes national standards for how PHI can be used and disclosed, while also giving patients important rights over their health information, such as the right to access their records and request corrections.
- **The Security Rule** focuses specifically on electronic PHI and requires organizations to implement administrative, physical, and technical safeguards to protect it from unauthorized access, breaches, or loss.
- **The Breach Notification Rule** requires organizations to notify affected individuals, regulators, and sometimes the public if sensitive health information is compromised.

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 stored, manipulated, or communicated on an electronic network.

Covered entities

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.

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.

HIPAA Security Rule updates in 2026

The HHS proposed a major modernization of the HIPAA Security Rule through a Notice of Proposed Rulemaking (NPRM) released in late 2024 and published in the Federal Register in January 2025. The final rule is expected around May 2026. The goal of the update is to strengthen cybersecurity protections for electronic protected health information (ePHI) in response to the sharp rise in ransomware attacks and large healthcare data breaches.

One of the most significant proposed changes is the removal of the distinction between "required" and "addressable" security controls in the old Security Rule. Under the pre-existing framework, some safeguards are mandatory while others are "addressable," meaning organizations can determine how or whether to implement them based on risk. The proposed rule would largely eliminate this flexibility and make nearly all implementation specifications mandatory. The proposed rule also introduces much more prescriptive cybersecurity requirements, including:

- Mandatory **encryption** of ePHI at rest and in motion.
- Mandatory **Multi-Factor Authentication (MFA)** and stronger access controls for access to ePHI system.
- Mandatory **risk assessment**, data inventory, and mapping of movement of ePHI.
- Mandatory **anti-malware** protections, vulnerability management and continuous monitoring.
- Mandatory **oversight of third party** and business associates.
- Mandatory **incident response**, resilience, and recovery requirements.

How Thales can help your organization comply with the 2026 HIPAA Security Rule updates

Thales cybersecurity products can directly support these requirements by helping organizations protect data, control access, and demonstrate compliance with the latest HIPAA Security Rule updates.

Mandatory encryption of ePHI both at rest and in transit

Thales Data Security solutions help organizations implement encryption across databases, files, and cloud environments, protecting sensitive healthcare data wherever it resides and while in transit without requiring changes to existing applications. This ensures that patient information remains protected even if systems are compromised.

Multi-Factor Authentication (MFA) and stronger access controls

The proposed rule places stronger emphasis on identity verification and access control, including the use of multi-factor authentication (MFA) for systems that handle healthcare data. Thales Identity and Access Management solutions solutions enforce strong authentication policies, support phishing-resistant MFA methods like FIDO2 security keys, and implement granular role-based access controls. These capabilities help ensure that only authorized users can access patient records and other sensitive information, reducing the risk of insider threats or credential-based attacks.

Risk assessment, data inventory, and mapping of movement of ePHI

Another key focus of the updated HIPAA Security Rule is visibility and monitoring of sensitive data. Thales solutions include capabilities for data discovery, classification, and activity monitoring, which help organizations identify where ePHI resides, track who is accessing it and where it goes. This visibility is essential for risk analysis, audit readiness, and rapid detection of suspicious activity that could indicate a data breach.

Continuous monitoring, anti-malware and vulnerability management

Thales solutions provide centralized logging, monitoring, and policy enforcement that help organizations demonstrate continuous oversight of personal data usage. They also monitor I/O and block suspicious activity before ransomware can take hold and use signature, behavioral and reputational analysis to block all malware injection.

Strong oversight of third parties and business associates

Thales solutions reduce risks from third parties such as cloud providers by controlling cloud encryption keys, ensuring complete separation of roles between cloud provider and data owner and monitoring anomalies before disrupting supply chain. In addition our identity & access management solutions enable delegated relationship management and fine-grained authorization of third-party users.

Incidence Response

Thales Application Security solutions inspect all traffic, detect and prevent web-based attacks, preventing DDoS and Bad Bot attacks with scalable attack traffic absorption provided by edge servers.

Mapping Thales capabilities to HIPAA requirements

Thales solutions simplify compliance and automate security reducing the burden on security and compliance teams. We help address essential control requirements for HIPAA addressing application security, data security, and identity & access management requirements across multiple categories.

- **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).
- **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 behavior 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.

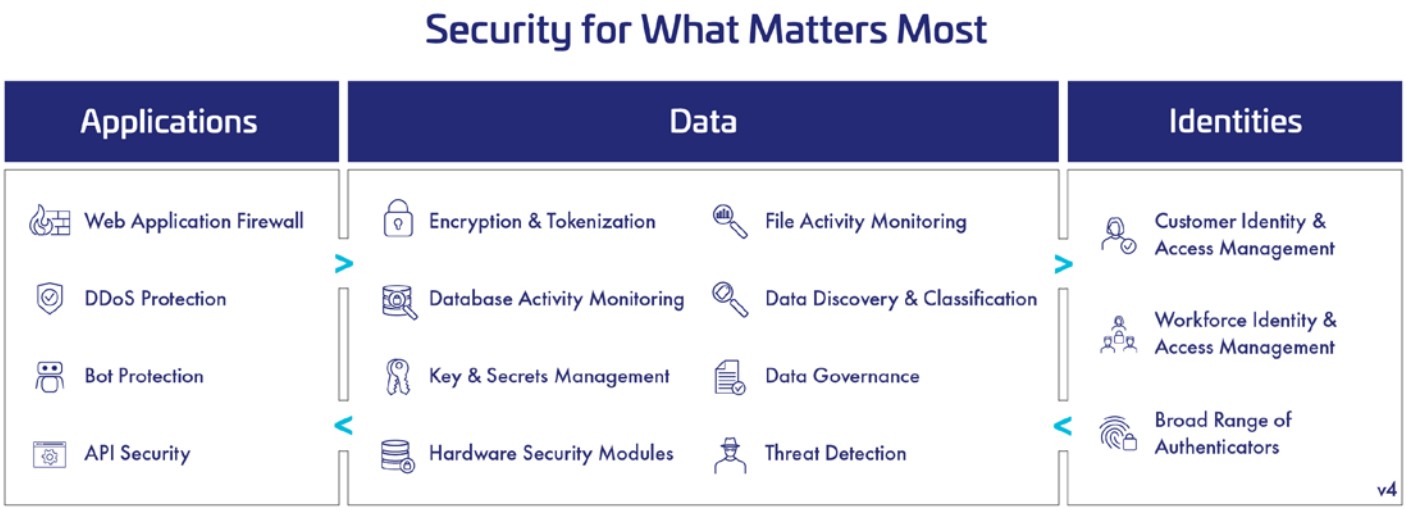
Mapping Thales capabilities to HIPAA requirements

Requirement	How Thales Helps	Solution Areas
164.306 Security Standards: General rules		
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.	**Data Security** Data Security Posture Management
164.308 Administrative Safeguards		
A, 1, B, 2: Risk Analysis Map ePHI flow through information systems. **A, 2: Identify potential risks and vulnerabilities to ePHI**	• Identify structured and unstructured sensitive data at risk across Hybrid IT. • Determine risk scores for data assets to assess potential risks. • Identify flow of sensitive data across multiple systems. • Discover and classify potential risk for all public, private, and shadow APIs and conduct API risk assessment.	**Application Security** API Security **Data Security Data** Discovery & Classification Data Risk Intelligence Database Activity Monitoring File Activity Monitoring
B, 1: Identify and respond to suspected or known security incidents	• Inspect all traffic, detect and prevent web-based attacks with WAF. • Prevent DDoS attacks with scalable DDoS attack traffic absorption provided by edge servers.	**Application Security** Web Application Firewall DDoS Protection
8, B, 1: Reduce risk from third party business associates	• 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. • Minimize privileges by using relationship-based fine-grained authorization. • Enable MFA for third-party users to thwart phishing attacks.	**Data Security** Cloud Key Management Transparent Encryption Database Activity Monitoring File Activity Monitoring **Identity & Access Management** Third-party Access Control Delegated User Management Externalized Authorization

Requirement	How Thales Helps	Solution Areas
164.312 Technical Safeguards		
A, i, ii, iv, v: Administrative and increased access privileges **vii: Data controls** **D Standard: Audit trail and system log controls** **ii: Administrative and increased access privileges**	• Limit the access of internal and external users to systems and data based on roles and context with policies. • Centralize access control over multiple hybrid environments in a single pane of glass • Prevent password fatigue with Smart Single Sign-On with conditional access. • Apply contextual security measures, terminate session or prevent logon based on risk scoring. • Enforce granular user access policies to sensitive data and secrets. • Enable complete separation of roles where only authorized users and processes can view unencrypted data. • Monitor access and assess risk to sensitive resources, data, and files. • Produce audit reports of all access events to systems, stream logs to SIEM	**Identity & Access Management** Workforce Access Management **Data Security** Database Activity Monitoring File Activity Monitoring Transparent Encryption
B, 1, 2, G: Encrypt all electronic protected health information at rest and in transit	• Protect data-at-rest, in use, and secrets across hybrid IT. • Protect data in motion with high-speed encryption. • Pseudonymize and mask sensitive information for production or tests. • Protect cryptographic keys in a FIPS 140-2 Level 4 environment. • Streamline key management in cloud and on-premises environments. • Manage and protect all secrets and sensitive credentials. • Maintain crypto-agility with products designed for post-quantum upgrade. • Secure execution with Confidential Computing.	**Data Security** Transparent Encryption Tokenization Key & Secrets Managemen Hardware Security Modules High Speed Encryption Confidential Computing
C 2, i: Anti-malware protection	• Use signature, behavioral and reputational analysis to block all malware injection attacks. • Detect and prevent cyber threats with web application firewall. • Monitor I/O and block suspicious activity before ransomware can take hold. • Prevent malicious software and users from accessing sensitive data.	**Application Security** Web Application Firewall Bot Protection **Data Security** Ransomware Protection Data Risk Analytics
F, 1, 2: Authentication **ii, A, B Multi-factor authentication**	• Enable MFA with the broadest range of hardware and software methods. • Build and deploy adaptive authentication policies. • Protect against phishing and man-in-the-middle attacks. • Risk-Based Authentication and PKI and FIDO Authenticators.	**Identity & Access Management** Multi-Factor Authentication Risk-Based Authentication
H: Vulnerability Management	• Vulnerability assessment and risk mitigation.	**Data Security** Vulnerability Management Data Risk Intelligence

Visibility and Control

Thales delivers a broad portfolio of complementary application security, data security, and identity & access management products to provide a comprehensive solution that helps address the HIPAA requirements. The portfolio delivers comprehensive data-centric security that protects data and all paths to it with platforms that reduce the complexity and risks of managing applications, data, and identities in the cloud.



Application Security Solutions

Web Application Firewall (WAF)

Modern web applications are mission-critical for most organizations in all business sectors, and protecting these apps is key for business continuity and resilience. The Imperva Web Application Firewall provides out-of-the-box security for web applications, detecting and preventing cyber threats, ensuring seamless operations and peace of mind. Our WAF solution protects against Open Worldwide Application Security Project (OWASP) Top 10 security threats, such as cross-site scripting, illegal resource access, and remote file inclusion, blocking attacks in real time. Our threat research team updates rules that are automatically pushed out daily to ensure our solution protects customers from the latest threats.

Distributed Denial of Service (DDoS) Protection

DDoS attacks are cybercrimes that attempt to force a website, computer, or online service offline. Imperva DDoS Protection provides comprehensive DDoS protection for websites, networks, DNS servers, and individual IPs. Our solutions have mitigated the largest attacks in history, immediately and without incurring latency or interfering with legitimate users. Our high-capacity global network holds more than six Terabits per second (6 Tbps) of scrubbing capacity and can process more than 65 billion attack packets per second. This global network of 44+ points of presence (PoPs), each outfitted with a DDoS scrubbing center powered by proprietary Behemoth custom technology, cloud-based WAF, advanced bot mitigation services and more, acts as a software-defined mesh network for optimal performance.

Bot Protection

The volume of automated threats on the internet is continuously rising, as bad bots account for over thirty percent of all internet traffic. Imperva Advanced Bot Protection safeguards mission-critical websites, mobile apps, and APIs from automated threats and online fraud without affecting the flow of business-critical traffic. It defends customers against web scraping, account takeover, scalping, transaction fraud, gift card fraud, denial of service, competitive data mining, unauthorized vulnerability scans, spam, click fraud, and web and mobile API abuse.

API Security

Whether developing applications in new cloud-native microservice and serverless architectures, automating business-to-business processes, or providing a back-end for mobile applications, APIs are essential to the modern enterprise. Through automatic discovery and continuous monitoring of API endpoints, Imperva API Security enables comprehensive API visibility for security teams – without requiring development to publish APIs via OpenAPI or by adding resource-intensive workflow to their CI/CD processes. Moreover, every time an API is updated, security teams can stay on top of the change, understand any new risks, and incorporate changes, which leads to faster, more-secure software release cycles. Imperva API Security enables security teams to keep pace with innovation without impacting development velocity.

Data Security Solutions

Data Discovery and Classification

A crucial first step to aligning with HIPAA is understanding where and how electronic PHI is stored, and who can access it. CipherTrust Data Discovery & Classification discovers and classifies data in all the data stores in an organization's data estate, from structured to semi-structured to unstructured across on-premises, hybrid, cloud, and multi-cloud environments. This visibility enables organizations to build a strong data privacy and security foundation.

Database Activity Monitoring

Continuous monitoring captures and analyzes all data store activity, in the cloud or on-premises, for both application and privileged user accounts, providing detailed audit trails that show who accessed what data, when, and what was done to the data. Our Database Activity Monitoring (DAM) solution unifies auditing across diverse on-premises platforms, providing oversight for relational databases, NoSQL databases, mainframes, big data platforms, and data warehouses. It also supports databases hosted in Microsoft Azure and Amazon Web Services (AWS), including PaaS offerings, such as Azure SQL and Amazon Relational Database Services (RDS). Detailed data activity is captured automatically, making it easier to fulfill audit requests.

File Activity Monitoring

Unstructured data, encompassing everything from Office documents to chat logs, Gen AI outputs, and medical images, now accounts for roughly 80 of enterprise information assets. Yet security tooling is still optimized for structured databases, leaving assets like emails and file shares unmonitored. Our File Activity Monitoring (FAM) solution closes this gap by enhancing visibility and control over unstructured data, enabling organizations to monitor file activity, detect misuse, and ensure regulatory compliance across their entire data estate. Thales FAM realtime access tracking, automated classification, and AI-driven insights, enable compliance, detect insider risks, and provide deep visibility into sensitive file activity—all through an intuitive dashboard and seamless deployment.

Data Risk Intelligence

In order to make effective data risk decisions, it is vital to have an accurate risk score that reflects your specific security tolerance and organizational goals. Our Data Risk Intelligence solution empowers organizations to accurately pinpoint the most critical data risks by severity and likelihood, enabling them to effectively prioritize risk mitigation. It delivers specialized insights derived from a wide-ranging set of data risk indicators through advanced analytics, encompassing user permissions, data source vulnerabilities, encryption status and suspicious activities, furnishing a specific risk score and clear-cut recommendations for necessary action.

Threat Detection

Threat detection is one of the most important capabilities to prevent or identify and respond to a cyberattack. Our Threat Detection solution monitors data access and activity for all databases providing the visibility needed to pinpoint risky data access activity for all users, including privileged users. Organizations can uncover hidden risks and vulnerabilities while creating reports to effectively communicate risk and ongoing activities. It delivers real-time alerting, user access blocking of policy violations, and cost-effectively retains years of data for auditing purposes.

Combining deep domain security expertise with machine learning (ML) allows organizations to identify suspicious user and computer system behaviors that violate security policies, practices, and peer group norms. Purpose-built detection algorithms instantly recognize active attack exploits and immediately send incident alerts.

Encryption

Encryption plays an important role in protecting data's confidentiality, integrity, and availability across its lifecycle: at rest, in-motion, and in use.

Data at Rest

Depending on your security requirements and infrastructure, different approaches can be used to protect data-at-rest in files, volumes, and databases. The CipherTrust Data Security Platform provides multiple capabilities for protecting data at rest in files, volumes, and databases. Transparent Encryption operates at the file system layer, delivering data-at-rest encryption with centralized key management, granular access controls, and data access logging to meet best practice requirements for protecting data. To protect the availability of data-at-rest from zero-day and privileged escalation attacks, ransomware protection uses real-time behavior monitoring to alert or block malicious activity before ransomware can take hold of data. Database protection at the database layer supports key management for native TDE use cases or the ability to do field or column-level encryption on databases. At the application layer, libraries for C and Java can be deployed, or solutions at the network layer can be used as a gateway to apply encryption without modifying the application code.

Data in Motion

Protecting data in-motion is essential to prevent eavesdropping, surveillance, and overt and covert interception of sensitive data. Thales High

Speed Encryption provides certified, 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, allowing customers to better protect data, video, voice, and metadata flowing between repositories. The network encryption solution has been proven to deliver maximum uptime in the most demanding, performance-intensive environments. It has near-zero latency and can operate in full-duplex mode at full-line speed while offering flexible and vendor-agnostic interoperability, meaning it's compatible with all the leading network vendors throughout your network.

Tokenization

Tokenizing or masking data reduces the cost and effort required to comply with internal security policies, industry frameworks, and regulatory mandates such as CMMC, the European Union's Global Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI-DSS). CipherTrust Tokenization permits the pseudonymization of sensitive information in databases so you can analyze aggregate data without exposing sensitive data during analysis. It offers application-level tokenization services in two convenient solutions that deliver complete customer flexibility: Vaultless Tokenization with Dynamic Data Masking and Vaulted Tokenization. Both solutions secure and anonymize sensitive assets, whether they reside in the data center, big data environments, or the cloud.

Key & Secrets Management

Centralized key management consolidates on-prem and cloud encryption keys so you can apply consistent security policies across multiple file servers, databases, applications, virtual machines, and cloud platforms. CipherTrust Key Management provides a greater command over your keys and simplifies key lifecycle management tasks while enhancing data security through consistent enforcement of key policies, fine-grained access control, and robust auditing and reporting of all key management and encryption operations.

Modern development trends, such as containerization, cloud transformation, DevOps, and automation, have contributed to a massive increase in the use of secrets (credentials, certificates, keys) for authentication, which can be vulnerable to cyber-attacks when not securely managed. CipherTrust Secrets Management protects and automates access to mission-critical secrets across DevOps tools and cloud workloads, including secrets, credentials, certificates, API keys, and tokens, to help security and governance teams reduce risks by streamlining security processes.

Hardware Security Modules

A hardware security module (HSM) is a dedicated crypto processor that protects the crypto key lifecycle. It acts as a trust anchor that protects the cryptographic infrastructure of some of the world's most security-conscious organizations by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. Thales Luna Hardware Security Modules 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. They are available on-premises, in the cloud as-a-service, and across hybrid environments.

Luna HSMs generate and protect root and certificate authority (CA) keys, supporting PKIs across various use cases. They sign the application code to ensure the software remains secure, unaltered, and authentic. They create digital certificates for credentialing and authenticating proprietary electronic devices for IoT applications and other deployments.

Identity & Access Management Solutions

Customer Identity & Access Management

Customer Identity & Access Management (CIAM) manages access for identities external to an organization such as the identities of customers, gig workers, suppliers, or partners. Thales OneWelcome Identity Platform provides a consistent identity experience across all customer touchpoints, allowing organizations to balance security and usability to enable a frictionless experience for customers at scale – regardless of their location, device, or application. The CIAM platform can handle the most complex local, national, and international data privacy and protection regulations and thereby enables organizations to thrive in complex regulated markets.

Workforce Identity & Access Management

A disproportionate number of data breaches start with unauthorized access of data and sensitive resources, credential compromise, and privilege abuse. Thales SafeNet Trusted Access is a cloud-based access management solution that makes it easy to manage access to both cloud services and enterprise applications with an integrated platform that combines single sign-on (SSO), multi-factor authentication (MFA), and scenario-based access policies. SafeNet Trusted Access provides a single pane view of access events across an organization's app estate to ensure that the right user has access to the right application at the right level of trust. SafeNet Trusted Access allows organizations to virtually (or logically) limit the access to confidential resources through use of MFA (including phishing-resistant authentication) and granular access policies.

Broadest Range of Authentication Solutions

Multi-factor authentication is an important new requirement of HIPAA and most other regulations and standards. Thales OneWelcome Authenticators include a broad range of hardware and software authentication methods and form factors for workforce and external users. These include phishing-resistant authentication capabilities such as CBA and FIDO, in addition to user-friendly smartphone-based authenticator app

called MobilePASS+. External users, like customers or partners, also have nuanced authentication needs. With the OneWelcome Identity Platform, organizations can enable both low-assurance and high-assurance authentication mechanisms, including SCA (Strong Customer Authentication) or use of FIDO Passkeys.

Conclusion

The HIPAA updates of 2026 dramatically raise the bar for privacy protection and protection of data for organizations handling large amounts of sensitive healthcare data. Drawing on decades of experience helping corporate entities and public enterprises adhere to compliance mandates, Thales offers a broad range of products and services that enable organizations to strengthen privacy protection, address the security requirements, streamline reporting obligations, and comply with the more stringent requirements of HIPAA.

Moreover, the Thales Cyber Security Products portfolio helps simplify compliance across multiple overlapping regulatory regimes in addition to HIPAA, such as GDPR and SOC 2, or standards such as ISO 27001, PCI DSS, or the NIST Cybersecurity Framework 2.0. Our portfolio delivers unparalleled centralized visibility and control over data, application, and access control security, helping automate security and compliance processes and reducing the burden on security and compliance teams.

About Thales

Thales is a global leader in cybersecurity, helping businesses, governments, and the most trusted organizations in the world protect critical applications, sensitive data, identities, and software anywhere, at scale — with the highest ROI. With more than 30,000 customers, including 58% of the Fortune Global 500, our solutions are deployed in 148 countries around the world. Through our innovative services and integrated platforms, Thales helps customers achieve better visibility of risks, defend against cyber threats, close compliance gaps, and deliver trusted digital experiences for billions of consumers every day.

THALES

CYBERSECURITY

Contact us

For contact information, please visit
cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com