

Using Encryption and Access Control for HIPAA Compliance

THALES

Introduction

Striking a balance between compliance and security is an issue faced by every organization that handles data. With new technologies emerging and regulations and enforcement shifting to address their requirements, change seems to be the only constant, making regulatory compliance an ongoing challenge. However, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules have remained largely unchanged since their inception. Sure, there have been some changes to these rules, but the more significant changes required by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) have been to enhance penalties against HIPAA violators and to require HIPAA covered entities to report breaches of protected health information (PHI) to affected individuals and the Office for Civil Rights (OCR). Following these developments, enforcement of HIPAA, which was seemingly nonexistent for several years after the effective dates of the Privacy and Security rules, is now in full swing. The mere threat of a breach investigation can put staff on edge, while a hacking or ransomware incident potentially can drive a healthcare provider out of business.

There is no HIPAA compliance seal of approval. But there is guidance published by OCR and other government agencies addressing various administrative, physical, and technical privacy and security measures that can be implemented to safeguard PHI. One way to determine current enforcement areas of focus is to review resolution agreements and other enforcement actions taken by OCR against organizations that have suffered a data breach. One topic that is generally mentioned in each such enforcement action, as either missing or insufficient, is the security risk analysis. Other commonly-cited areas of noncompliance include staff improperly accessing information or revealing information to the wrong party, lack of updated (or any) business associate agreements, and loss or theft of laptops and smart phones that are not encrypted. Some hacker activity is mentioned, but most scenarios appear to arise from acts or omissions of those closest to the organization, the “insiders.” Although no fine or settlement agreement has yet arisen out of a ransomware type attack, ransomware has gained considerable attention since OCR issued statements that such attacks are deemed to represent a breach of PHI due to the entity’s loss of control over its data. These attacks can generally be traced back to “the insider” clicking on a link or otherwise providing a hacker with an initial point of entry into the organization’s information system. According to 451 Research, 47% of US healthcare organizations have suffered a breach, 20% of these within the last year¹.

So how does an organization protect itself from insiders—the very people it needs to be able to trust the most? The answer is simple: organizations must emphasize the protection of the very object of the HIPAA law itself—the information about the patient.

Fortrex’s evaluation of Thales eSecurity’s data security products has revealed that they are capable of supporting an organization’s goals for achieving the encryption, access control, logging and monitoring technical requirements of HIPAA when implemented within an overall HIPAA compliant security architecture. Since every organization is unique in its implementation of the administrative, technical, and security requirements of HIPAA, please carefully review the recommendations in this paper within the context of the technical architecture of the existing or prospective environment. Better still, conduct a security risk analysis, which is a requirement of the HIPAA Security Rule.² This will ensure that your organization is deploying the right controls, at the right time, in the right way to address the risks it faces. While this paper does not provide detailed instructions for how to configure Thales products within your environment, it illustrates the complementary features of Thales eSecurity’s solutions to secure PHI in accordance with the HIPAA implementation requirements.

HIPAA Requirements

On January 25, 2013, the final HIPAA Omnibus Rule was published. It expanded to business associates the obligation to comply with certain administrative, technical and physical security controls to safeguard the confidentiality, integrity, and availability of PHI. As noted above, the HITECH Act and the Omnibus Rule enhanced enforcement of the HIPAA Privacy, Security and Breach Notification Rules. Although HIPAA has been in place since 1996, it is not the only legislation that requires data privacy or security safeguards. The FTC issued the Health Breach Notification Rule on February 22, 2010 that requires some organizations not covered by HIPAA to notify customers when a breach of individually identifiable electronic health information has been recognized. This rule identified the need for security and privacy rules among vendors of personal health records (PHRs), PHR-related entities, and third party service providers to PHRs. While all of these regulations have a variety of requirements, this paper focuses on the relevant requirements addressed by Thales' data security solutions.

Security professionals, covered entities, business associates, clearing houses, service providers, application developers, hardware manufacturers and converged infrastructure vendors are working to address the increasing demands for data privacy and security in the healthcare industry. Virtualization and cloud computing can create additional challenges in achieving compliance with HIPAA/HITECH, but they do not inherently prevent compliance.

The HIPAA Security Rule implementation specifications are divided between "required" and "addressable" components. While a "required" specification clearly means that the organization must fully implement the particular specification, the meaning of "addressable" has been misinterpreted. The Department of Health and Human Services (DHHS) has provided guidance for "addressable" specifications in its "HIPAA Administrative Simplification Regulation Text", March 2013: "When a standard adopted in 164.308, 164.310, 164.312, 164.314, or 164.316 includes addressable implementation specifications, a covered entity or business associate must: (A) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting electronic protected health information; and as applicable to the covered entity or business associate."³ The text goes on to state that the organization must either implement the specification if it is reasonable and appropriate, or implement an equivalent alternative measure, and document the security measures or justification accordingly.

What is "reasonable and appropriate"? 45 CFR Section 164.308 requires covered entities to perform an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI (ePHI). Managing these risks and ensuring that applicable security controls are in place are part of a solid risk analysis, which forms the basis for determining which controls are reasonable and appropriate within a given environment.

The HIPAA Security Rule addresses the technical safeguards in 45 CFR Section 164.312. It begins by requiring access controls for all systems that maintain ePHI. It further requires that organizations restrict access to such ePHI based on each user's "need to know." The law requires that only those individuals, systems and applications that require the data in order to perform their job functions be provided access to ePHI and to the systems that contain ePHI.

In order to further restrict access to ePHI, the HIPAA Security Rule recommends that companies implement encryption and decryption procedures. At the time that the law was enacted, these encryption and decryption technologies were considered to be addressable specifications. Combined with the requirements to perform a risk analysis and to implement controls deemed reasonable and appropriate, it is easy to see how the anticipated growth in technology was considered in the original version of the rules. Specifically, the Security Rule required the following technical safeguards:

Category	Technology	Required or Addressable
Access Controls	Unique User ID	Required
	Emergency Access Procedures	Required
	Automatic Log-off	Addressable
	Encryption and Decryption	Addressable
Audit Controls		Required
Integrity	Authenticate Electronic PHI	Required
Person or Entity Authentication		Required
Transmissions Security	Integrity Controls	Addressable
	Encryption	Addressable

Note that many of the provisions that are deemed “addressable” are controls based on technology that was either expensive, complex, or not widely available in the 1990s. The HIPAA Security Rule was designed to be scalable to permit companies to conduct a risk analysis appropriate to their size and resources to see if certain requirements could be met with an alternative solution. Today, many of those “addressable” requirements, particularly encryption, are proven, relatively inexpensive, and widely available, and they provide more manageable protection than was the case in the late 1990s.

Each covered entity and business associate is required to perform an organizational risk analysis. This risk analysis provides the basis whereby an organization determines whether encryption of data at rest, as an addressable implementation specification (164.312 (a)(2)(iv)), is reasonable, appropriate, and cost effective for the organization. Access controls, as required implementation specifications, must be implemented and must support the overall goal of the legislation to ensure the confidentiality, integrity, and availability of the protected health information. An examination of current action taken by OCR to investigate and penalize organizations without these controls reveals that these controls are taken seriously as a means to avoid a breach. Simply not addressing gaps or deficiencies in compliance has become unacceptable and expensive.

Phase 2 of the HIPAA Privacy, Security, and Breach Notification Rules Audit Program

The HITECH Act required OCR to audit the HIPAA compliance of covered entities and business associates that create, receive, maintain or transmit PHI. OCR's initial audit program, developed and carried out in 2011 and 2012, assessed the compliance of 115 covered entities. The audit results were reviewed, and changes were incorporated into the overall audit program. Significant findings included that most health care providers did not have a complete or accurate risk analysis, mobile device management lacked adequate controls, access to PHI was not well managed, incident procedures were not documented or tested, and encryption had not been addressed. Smaller entities accounted for a disproportionate share of the Phase 1 audit findings. These results were used to develop the "Phase 2" audit program.

On July 11, 2016, OCR launched Phase 2 of its HIPAA Audit Program by sending letters to 167 covered entities, notifying them that they had been chosen to participate in desk audits of their compliance with the HIPAA Privacy, Security, and Breach Notification rules. OCR identified the Phase 2 audits as "primarily a compliance improvement activity" to enable OCR to better understand current compliance efforts and to determine what technical assistance to develop to assist entities in monitoring their HIPAA compliance programs and to prevent breaches. Nonetheless, OCR stated that it could "decide to open a separate compliance review in a circumstance where significant threats to the privacy and security of PHI are revealed through the audit."

Because OCR's Audit Program will be a permanent part of OCR's enforcement activity, with some of the money recovered from settlement agreements to be used to fund the Audit Program, entities should continue to evaluate their compliance with HIPAA's requirements even if they were not selected for a Phase 2 audit. Additionally, OCR retains separate, broad authority to open compliance reviews in a circumstance where, through the audit process, significant threats to the privacy and security of PHI are revealed to exist at a covered entity or business associate.

HITECH Enforcement Provisions

For several years after the adoption of HIPAA, enforcement of the law was minimal. In fact, 2014 only saw 6 resolution agreements and 2015 saw 6 resolution agreements, but 2016 saw 12 resolution agreements. The Enforcement Provisions of HITECH directly addressed the resulting lax compliance efforts by strengthening both the civil and criminal penalties associated with a violation of HIPAA. The Enforcement Rule delineates four categories of violations and their corresponding fines. The following table from the HITECH Act Enforcement Interim Final Rule demonstrates how organizations will be fined for failure to comply. HIPAA/HITECH enforcement actions fall under the purview of the Federal Trade Commission (FTC) and the Health and Human Services Office of Civil Rights (HHS OCR).

Violation Category	Each Violation	All Violations of Identical Provisions in a calendar year
Did not know	\$100 – \$50,000	\$1,500,000
Reasonable Cause	\$1,000 – \$50,000	\$1,500,000
Willful Neglect – Corrected	\$10,000 – \$50,000	\$1,500,000
Willful Neglect – Not Corrected	\$50,000	\$1,500,000

In 2016, OCR assessed \$23.5 million dollars in fines against covered entities and business associates. This was nearly four times the amount assessed in 2015. Based on cases released in the first half of 2017, this trend of ever-increasing fines could continue. Here are a sample of fines imposed from 2016 and 2017 and the underlying HIPAA violations:

- Impermissible disclosure of unsecured ePHI, stolen unencrypted laptop – \$2.5 million fine
- Impermissible disclosure of ePHI, lack of access control, lack of access reviews – \$5.5 million fine
- Lack of encryption on mobile devices, lack of access controls, insufficient physical security – \$3.2 million fine
- Malware infection – \$650,000 fine
- Unencrypted/publicly accessible files – \$2.14 million fine
- Unencrypted mobile devices, lack of risk assessment, lack of BAA – \$5.55 million fine

The underlying message of these enforcement examples is clear: covered entities and business associates must conduct a security risk analysis to understand the organization's security posture; properly limit access to PHI; review auditing controls as often as possible; and encrypt data wherever possible to protect it against theft, loss or interference due to malicious activity.

How Thales eSecurity Supports HIPAA Compliance

Thales eSecurity solutions help organizations strengthen their compliance postures in three important areas:

- Rendering ePHI unusable, unreadable or indecipherable to unauthorized individuals
- Restricting access to ePHI
- Auditing access to ePHI

Rendering ePHI unusable, unreadable, or indecipherable to unauthorized individuals

The HIPAA Security Rule provides that organizations should protect ePHI through the implementation of encryption. Often, organizations deploy various solutions to provide protection for different applications, data types and infrastructures, which can prove to be very complex. For example, many environments have a variety of applications, file types and even operating systems. While some types of data, such as credit card data or social security numbers found in databases, can be readily located and protected, the unstructured data frequently found in electronic health records, medical images and other files dispersed across multiple environments can be more difficult to identify and protect. Organizations that contain “big data” environments, or have connected “Internet of Things (IoT)” environments, must pay particular attention to encryption requirements.

An additional challenge lies in controlling access to ePHI, as IT administrators with no-need-to-know about the data often have full access. The best way to meet these requirements is through data-at-rest encryption or tokenization of data, access control and audit logs.

Thales eSecurity enables organizations to address the requirements in the HIPAA Security Rule with solutions appropriate to their environments and implementations. File and folder level encryption, access controls and data access monitoring ensure that only authorized users and services can encrypt and decrypt protected data at the system level – and do so while avoiding re-coding applications or integrations. Support includes limiting access for administrators and users of big data environment well as Docker containers. Application encryption and tokenization offerings enable organizations to limit visibility of, and access to, ePHI at the next level up - within applications.

Encryption was first introduced by HIPAA as an “addressable” requirement. This meant that organizations were required to perform a risk analysis to determine if encryption was an appropriate control. If the same level of protection could be garnered through a different technology or process, then organizations had the ability to implement that “compensating control.” However, with the advent of the breach notification provisions in HITECH, deploying encryption is expected to become more critical. In fact, encryption provides a “safe harbor” to breach notification if, in the event of a compromise of ePHI, the organization can state that the information has been rendered “unusable, unreadable, or indecipherable to unauthorized individuals.”⁴

Thales eSecurity's Vormetric Data Security Platform also overcomes the challenge of securing heterogeneous data types. While many encryption solutions provide protection only for structured data – those found in databases or in other easily identifiable data stores – the very definition of ePHI renders those solutions moot. ePHI is defined by HIPAA/HITECH as any information that is “(a) created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse”; and (b) “relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”⁵ This definition could include a vast array of different file types (audio files, graphic files, movies, etc.) that reside in varying locations and applications across a widely dispersed network environment.

Restricting Access to ePHI

Thales eSecurity enables compliance with HIPAA/HITECH access control requirements by offering organizations the ability to layer additional access control functionality beyond the native file system and within applications using solutions from its Vormetric Data Security Platform of products. Thales' Vormetric Transparent Encryption solution works at the file system level and includes access controls that follow the least privilege model. Controls include who, what, where, when and how data may be accessed for permitted users. System administrators can perform their work without the ability to see sensitive data – data is not decrypted for them unless specifically authorized by policy. Meta-data can remain in the clear to allow required systems management and all data access activities can be logged and linked to SIEM systems for analysis of permitted access patterns, and denied access attempts. This protection also extends to big data environments with encryption and access controls for Hadoop admins and users, as well as to container environments.

In addition, the Vormetric Data Security Platform offers additional solutions that enable access controls at the application level. Application Encryption enables developers to map access control to data within their applications to application user roles – allowing equivalent controls for application administrators and users. Tokenization offerings enable call center, quality assurance, development and other use of healthcare records without exposing ePHI, replacing sensitive data with tokens.

Auditing Access to ePHI

A critical requirement is the ability to prove compliance to auditors by showing granular audit logs that track successful and failed data access to protected data. At the file system and volume level, proving compliance to auditors is easy with Vormetric Transparent Encryption. The solution includes standards-based syslogs that capture successful and failed user and application data access attempts with granular detail. This also extends to access by Hadoop-based big data environment and container users with extensions of Vormetric Transparent Encryption. In addition, these logs are easily shared with security information and event management (SIEM) Systems to accelerate the detection of insider abuse, advanced persistent threats, or the presence of a hacker attempting to access data.

Thales eSecurity Controls and Support Matrix

The following table provides additional details on the specific HIPAA requirements that are met by the Vormetric Transparent Encryption and other Vormetric Data Security Platform offerings. The table only lists those requirements that were considered either applicable or supported, and not the entire HIPAA Rule. Healthcare providers, business associates and any other entities covered by the requirements of HIPAA, the HITECH Act and the Omnibus Rule should always consult with their own auditors or risk assessors to determine the scope of controls applicable to them.

REQUIREMENT DESCRIPTION

Risk Management: Good risk management processes include timely and informative reports that are available to the right people at the right time. Reporting should also draw upon data over time – in seconds, minutes or months, so that trending of risk events can be managed. Some attacks slowly develop over time and good reporting and analytics are essential. As part of the comprehensive risk analysis, the organization must address whether encryption of data at rest, as an addressable implementation specification, is reasonable, appropriate, and cost effective.

THALES eSECURITY CAPABILITIES

The Vormetric Data Security Platform provides detailed security intelligence on who, what, when and how data was accessed at the file and volume level with detailed logging of access at the File System or Volume level for locations protected with Vormetric Transparent Encryption (VTE). All read/write requests to sensitive data are tracked with security compliant audit records. Policies allow for monitoring of all access to sensitive data, including access by privileged users. Logs showing security administrators actions for creating, updating and changing encryption policies and access control actions are also available from the Vormetric Data Security Manager (DSM). In addition, policy can be set in the DSM to send alerts associated with activities that require special monitoring. Reporting tools provide the ability to analyze logs generated by VTE agents and DSM. Also included are pre-built integrations and displays for major SIEM systems.

Vormetric audit logs can be stored in the DSM or in an organization's SIEM system or other log collection solutions for trending and correlation.

These audit logs can provide visibility and continuously monitor the risk of ePHI or PII data being accessed in the environment. When these logs are used with a SIEM, it becomes quicker and easier to identify compromised accounts and malicious insiders.

REGULATION REFERENCE

164.308(a)(1)(ii)

- Risk Analysis
- Risk Management

REQUIREMENT DESCRIPTION

Access Management: Access management should consist of authorization of users, de-registration of users, and strong authentication of the user. It is this point: the human-to-machine bridge that connects the “unknown” to the “known” in a technical environment.

THALES eSECURITY CAPABILITIES

Encryption and access control will not suffice to protect sensitive data unless the architecture includes an operations environment that controls insiders such as privileged users. In order to reduce the risk of a malicious administrator from compromising the protected data, the Vormetric Data Security Platform creates a management environment with strong separation of duties for Vormetric platform products. A strong separation of management duties assures that no one person has complete control and ability to compromise security policies that are enforced by the Vormetric platform.

The Vormetric Data Security Platform requires administrators of the system to be authenticated using a unique user ID and password. The tasks an administrator can perform are dependent upon their administrator type and provide the necessary segregation of duties. In addition, the Vormetric Management Console can enforce strict password rules and timeout login sessions.

The Vormetric platform supports Access Management in a number of ways.

Thales' Vormetric Transparent Encryption

Vormetric Transparent Encryption adds a layer of access control on top of the native operating system access control at the file system or volume level. It also can harden the access control defined at the OS layer and prevent root administrators and privileged users from accessing or viewing ePHI or PII. The solution enables least privilege access without interfering with normal administrative operations based on both LDAP/Active Director and system level roles and groups.

Vormetric Transparent Encryption can protect privileged users or any unintended users from viewing and accessing ePHI and PII using its encryption and access control methods. The solution provides the ability to create granular policies to control access, such as who and what process can apply encryption keys to encrypt and decrypt ePHI and PII.

These capabilities also extend to Hadoop-based big data environments as well as to Docker containers. For Hadoop environments encryption and access controls also apply to Hadoop users and administrators. When Vormetric Container Security is added to Vormetric Transparent Encryption, Docker user and administrator access controls can also be added for data stored both within Docker containers and in linked storage environments.

Cloud Infrastructure as a Service (IaaS) environments are also supported with access policies and encryption key management available in the cloud, or locally within an organization's data center.

The solution not only generates audit information for unintended direct access to ePHI/PII, it also generates audit information on operational functions such as login/logout, policy creation, deletion or edits, backups, and user administration. In addition, policy can be set in the DSM to send alerts associated with activities that require special monitoring. Integration with SIEM tools can also be used to generate alerts for providing integrity monitoring for ePHI/PII under its control. Pre-built integration and dashboards are available for many SIEM systems.

Thales' Vormetric Format Preserving Encryption

Thales' Vormetric Format Preserving Encryption (FPE) enables organizations to extend access controls into the next level up – within applications. Encryption provides enforcement for policies set within the application by developers and application administrators.

Thales' Vormetric Tokenization with Dynamic Data Masking

Enables organizations to control who is able to see ePHI/PII either stored in databases or for applications such as call centers or telemarketing organizations, replacing protected data with tokens. Controls can be applied by the application or by role within the organization.

REGULATION REFERENCE

164.308 (a)(4)(ii)(B,C)	• Access Authorization and, Establishment, and Modification
164.308 (a)(5)(ii)(C)	• Login Monitoring
164.312 (a)(2)(i)	• Unique User ID
164.312 (a)(2), ii)	• Emergency Access Procedure
164.312(a)(2)(iii)	• Automatic Logoff
164.312(c)(1,2)	• Integrity and authenticity of ePHI

REQUIREMENT DESCRIPTION

Encryption, Decryption: Data that has been encrypted is generally accepted as unreadable during that state. While not specifically required by HIPAA, some organizations require that data be encrypted to meet certain standards. Some organizations even go so far as to provide “safe harbor” to their partners when data remains in the encrypted state.

THALES eSECURITY CAPABILITIES

The Vormetric Data Security Platform supports a number of encryption solutions.

- Vormetric Transparent Encryption (VTE) supports file level and volume level encryption that expands encryption beyond a single file or a database column. VTE manages access to the encrypted data independent from the operating system’s access control. While integrated with a customer’s LDAP or Active Directory for authentication, access to decrypted data is based upon rules managed and administered within the Vormetric Data Security Manager. Cryptographic keys are not tied to user accounts, but are contained within the Vormetric system. The solution performs the encryption/decryption functions for file systems and volumes, as opposed to granting authorized and authenticated users access to the key. See the following requirement for Key Management.
- Vormetric Container Security extends VTE capabilities to encrypt data stored within containers and in underlying storage environments.
- Vormetric Application Encryption enables database column or file level encryption controlled by applications. Libraries provide fast access for developers to encryption capabilities. Cryptographic keys are managed by the Vormetric Data Security Manager.

REGULATION REFERENCE

164.312 (a)(2)(iv)	• Encryption and Decryption
164.312 (e)(2)(ii)	• Encryption
164.312(e)(2)(i)	• Integrity
164.312(c)(2)	• Mechanism to authenticate electronic health information (not altered or destroyed)

REQUIREMENT DESCRIPTION

Key management: Considered to be the “keys to the kingdom”, effective key management and protection must be demonstrated to support the encrypted state of data.

THALES eSECURITY CAPABILITIES

The user must document the key management processes used within their organization and ensure that key custodians understand and acknowledge their responsibilities.

The Vormetric Data Security Platform ensures cryptographic keys are centrally generated and stored by the DSM for all Vormetric platform applications. The actual keys are never visible to anyone, including key custodians or systems administrators.

The Vormetric platform restricts access to keys and key management activities by managing access within the Vormetric DSM, which decouples access rights from central access managements systems such as Active Directory, thus restricting access by privileged users such as system administrators and root unless explicitly granted within the DSM.

The Vormetric’s Data Security Manager architecture is designed for strong key management using a secure web management console:

- Cryptographic keys are centrally generated by the DSM appliance and are fully compliant with FIPS standards.
- Clear text keys never leave the DSM. When keys are distributed to agents, they are encrypted with a onetime-use AES 256 key and sent over a mutually authenticated TLS connection.
- Manual clear-text cryptographic key management is not required by the Vormetric platform. Custodians can create keys, but key values are not visible to the custodian. The DSM protects keys from any one person having access to key material by following a “no knowledge” and configurable split knowledge/dual control policies.
- Access control policies defined within the DSM control access to key creation and other key management activities, restricting access to authorized key custodians only.
- The DSM supports an “m of n” sharing scheme for backing up keys. A specific number of shares must be provided in order to restore the encrypted contents of the DSM archive into a new or replacement DSM.

The Vormetric Data Security Platform encrypts the data encryption keys with an AES 256-bit key. This encrypted key is stored securely on the DSM, which is separate from the location where the data encryption key is used. If the option to cache data encryption keys on the local server is selected, in order to eliminate network latency, the local keys are also encrypted with an AES 256-bit key.

REGULATION REFERENCE

164.312 (a)(2)(iv)
164.312 (e)(2)(i)

- Encryption and Decryption
- Integrity Controls

REQUIREMENT DESCRIPTION

Logging – Audit Controls: If not encrypted, and/or during the unencrypted state of data where it is human readable, it is required that data that has been read, accessed, or altered by a human must be tracked to create an audit trail. Logging of access to data must be retained. This logging of access can apply to:

- User access/network
- Program access/application layer
- Database administrator access
- Third party access
- Management review of logs

THALES eSECURITY CAPABILITIES

Vormetric Transparent Encryption provides logging of access at the File System and Volume level. All read/write requests to sensitive data is tracked with compliant audit records. User controlled policies allow for monitoring of all access to sensitive data, including access by privileged users. Reporting tools provide the ability to analyze logs generated by the agents and DSM. In addition, policy can be set in the DSM to send alerts associated with activities that require special monitoring.

Vormetric audit logs can be stored in the DSM or in an organization's SIEM system or other log collection solutions.

The Vormetric platform provides a detailed auditing at the File System level, by generating audit entries that include:

- Username and group membership
- Type of event
- Date and time
- Success or failure indication. In the case of a permitted action, the event data also includes whether the access was to clear text or to encrypted data
- Origination of the event
- Host and the full path to the file that was the target of the access request

The solution generates log reports for monitoring of daily activity. In addition, the solution can generate audit information for unintended direct access to ePHI/PII and can be configured to generate alerts thus providing integrity monitoring for ePHI/PII under its control.

The DSM can be configured to synchronize with an NTP server for accuracy of date/time, and can provide audit logs of security administrator activity.

REGULATION REFERENCE

164.312 (b)

- Audit Controls

REQUIREMENT DESCRIPTION

Monitoring: To support ongoing monitoring of access to ePHI/PII, organizations are required to ensure that access to ePHI/PII is appropriate. This access review will include not only the direct access obtained by anyone accessing the record, but it may also include system-based access.

THALES eSECURITY CAPABILITIES

Vormetric Transparent Encryption provides logging of access at the File Systems level. All read/write requests to sensitive data is tracked with compliant audit records. User controlled policies allow for monitoring of all access to sensitive data, including access by privileged users. Reporting tools provide the ability to analyze logs generated by the agents and DSM. In addition, policy can be set in the DSM to send alerts associated with activities that require special monitoring.

Vormetric audit logs can be stored in the DSM or in an organization's SIEM system or other log collection solutions.

REGULATION REFERENCE

164.308 (a)(1)(ii)(D)

- Information System Activity Review

REQUIREMENT DESCRIPTION

Security Incident Management: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

THALES eSECURITY CAPABILITIES

Vormetric Transparent Encryption supports this requirement by providing detailed logging of access at the File Systems level. All read/write requests to sensitive data is tracked with compliant audit records. User controlled policies allow for monitoring of all access to sensitive data, including access by privileged users. Reporting tools provide the ability to analyze logs generated by the agents and DSM. In addition, policy can be set in the DSM to send alerts associated with activities that require special monitoring.

The audit records contain information to track access back to a host machine, directory, file or resource accessed, specific user, user group, policy invoked, application and time.

Vormetric audit logs can be stored in the DSM or in an organization's SIEM system or other log collection solutions.

REGULATION REFERENCE

164.308 (a)(6)(ii)

- Response and Reporting

REQUIREMENT DESCRIPTION

Disaster Recovery Plan, Data Backup Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.

THALES eSECURITY CAPABILITIES

Although the Vormetric Data Security Manager does not store ePHI/PII directly on its system, the Vormetric Data Security Platform supports the ability to securely backup the configurations of the DSM for disaster recovery, as well as the ability to configure the solution in a High Availability configuration.

High-availability clustering configurations can span across Local Area Networks (LAN) or across geographies over Wide Area Networks (WAN). This clustering capability ensures high availability, fault tolerance, and load balancing across hardware DSMs or virtual machine DSM instances.

Back up of data encryption keys, policies, administrator accounts, and agent settings are easily and securely archived offline. For additional security, these archives are encrypted with a Backup Encryption Key that is split into parts and distributed to a configurable number of custodians. This approach ensures the DSM configuration is archived, but no single administrator can make use of the archive to exploit its contents.

Since the agents run independently, even loss of connection to the DSM will not take data offline. All encryption and access policies will remain intact and active to assure business continuity until network access is restored. In the case of a DSM hardware failure, the DSM cluster will continue to operate and a bare metal DSM replacement is fast and easy to accomplish.

The DSM uses an “n of m” sharing scheme where a secret is generated in m parts, or shares. A specific number of shares (n) must be provided in order to access the DSM and perform a DSM backup or restore operation. For example, a secret can be divided into six shares (m) and six individuals each receive one share. The required number of shares (n) can be set to three. This requires any combination of three of the six individuals to provide their shares before an administrator can perform a DSM backup or restore operation.

REGULATION REFERENCE

164.308 (a)(7)(i)

- Contingency Plan

REQUIREMENT DESCRIPTION

Removable media support: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.

THALES eSECURITY CAPABILITIES

While Vormetric Data Security Platform solutions do not directly apply to the specific tenets of this requirement, data that is copied outside of authorized processes controlled via Vormetric policies would be encrypted and unusable.

While not directly supporting this requirement, the Vormetric platform supplements other controls introduced to render retired hard drives or removable media unreadable. Should data not be adequately cleaned from media, the data will not be viewable unless the Vormetric Data Security Manager is available to authorize the decryption of the data on that media.

REGULATION REFERENCE

164.310 (d)(1)

- Device and Media Controls

REQUIREMENT DESCRIPTION

Security Reminders: Organizations should receive periodic security updates.

THALES eSECURITY CAPABILITIES

Thales eSecurity supports this requirement differently depending on whether a customer wants security reminders directly related to the Vormetric product or to the data that it protects.

Thales eSecurity customers can sign up for updates and alerts related to the Vormetric Data Security Platform.

The Vormetric platform has the ability to alert on critical events, such as unauthorized access to ePHI/PII that is protected by Vormetric Transparent Encryption. The log information can be stored local or integrated with 3rd party SIEM tools for further correlation, analysis and alerting.

REGULATION REFERENCE

164.308 (a)(5)(ii)(A)

- Security Reminders

Thales eSecurity Solutions for HIPAA/HITECH Compliance

The following sections provide additional detail about Thales eSecurity's data encryption, encryption key management, access control and security intelligence solutions that help covered entities strengthen compliance with HIPAA/HITECH.

The Vormetric Data Security Platform Solutions

Thales eSecurity's Vormetric Data Security Platform of solutions puts control in the health care administrator's hands by enabling encryption of ePHI and providing capabilities to control which users and applications can access and view that data. The Vormetric Data Security Platform is a comprehensive and extensible platform for delivering data at rest security across physical, virtual, big data and cloud environments. It offers centralized policy management and data-centric security for a broad range of solutions.

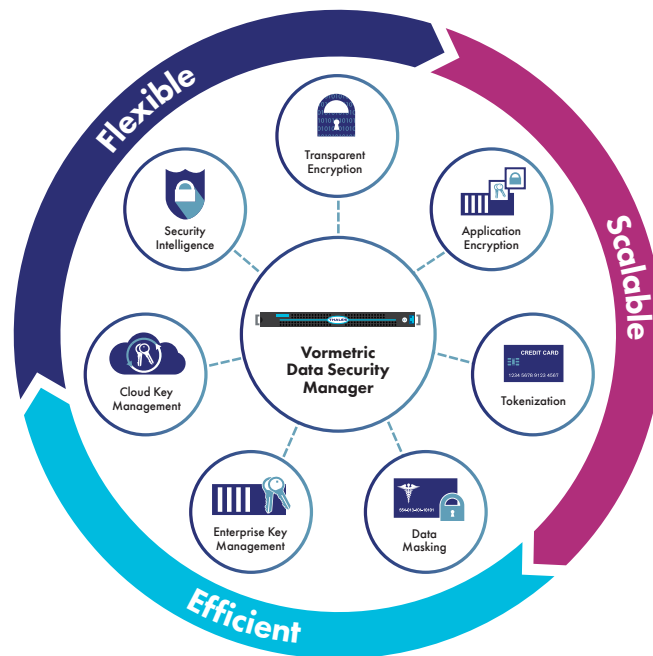


Figure 1: Thales eSecurity's Data Security Solutions

Vormetric Data Security Platform Components

Products leveraged in this HIPAA/HITECH solution include:

- Vormetric Data Security Manager (DSM)
- Vormetric Transparent Encryption (VTE)
- Vormetric Container Security
- Vormetric Application Encryption
- Vormetric Tokenization with Dynamic Data Masking

Data Security Manager

The Vormetric Data Security Manager integrates key management, data security policy management, and audit logging for all of Thales' Vormetric products. This enables data security administrators to easily manage standards-based encryption across all data security controls provided by the platform including solutions that support Linux, UNIX, and Windows operating systems in both centralized and geographically distributed physical, virtual, cloud, big data and container environments. Clustering DSMs provides high availability and scalability to tens of thousands of protected servers.

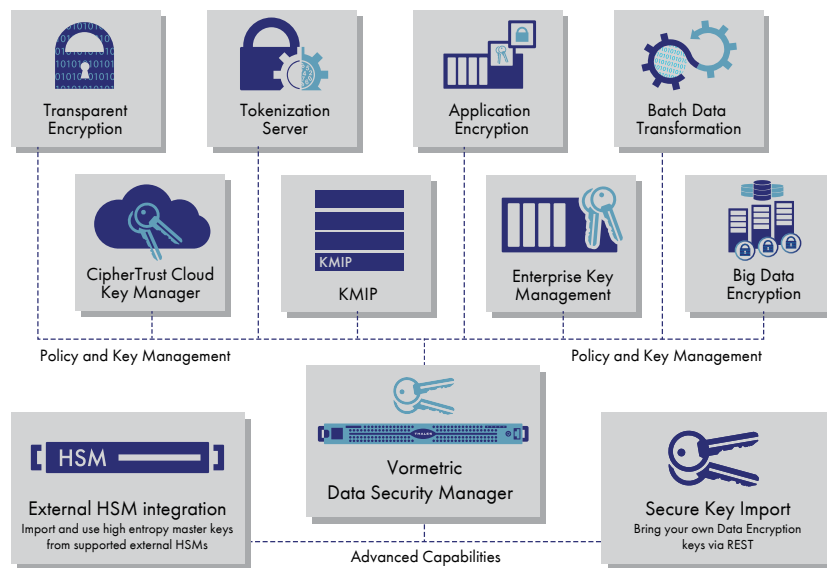


Figure 2: The Vormetric Data Security Manager provides common policy and key management controls for the entire Vormetric platform of products.

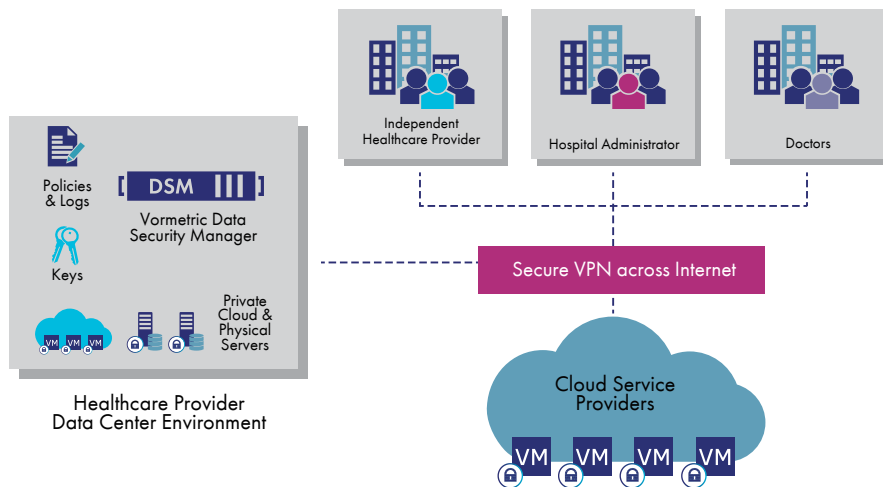


Figure 3: Controlling and Securing PII/PHI Data in the Cloud and On Premises

In support of HIPAA/HITECH requirements, the DSM can enforce strong separation of duties by requiring the assignment of key and policy management to more than one data security administrator. In this manner, no one person has complete control over the security of data. The DSM is accessed from a secure web-management console, CLI or through APIs.

The DSM deployment is flexible because it is available as a physical or virtual appliance. The virtual appliance can be deployed on premises or in the cloud. Either deployment model can be used for compliance to the HIPAA/HITECH requirements. It is important to note that the DSM is the key and policy manager and ePHI is never passed through it.

The DSM is available in the following form factors:

- A hardware appliance, 2U rack-mountable, with FIPS 140-2 Level 2 certification
- A hardware appliance, 2U rack-mountable, with integrated HSM, FIPS 140-2 Level 3 certification
- A hardened virtual appliance, which can run on-premises or in the cloud
- As a service through AWS Marketplace, Azure Marketplace

Vormetric Transparent Encryption

Vormetric Transparent Encryption enables data at rest encryption, privileged user access control and the collection of audit logs without re-engineering applications, databases or infrastructure. Vormetric Transparent Encryption requires file system agents that are installed above the file system logical volume layers. The agents perform the encryption, decryption, access control, and logging. The agents maintain a strong separation of duties on the server by encrypting files while leaving their metadata in the clear. This unique feature limits privileged users (i.e. root, system, cloud or storage administrators) from accessing data while preserving their ability to perform their day-to-day administrative responsibilities. Vormetric agents are installed on each server where data requires protection. The agents are specific to the OS platform and transparent to applications, databases (including but not limited to Oracle, IBM, Microsoft, Sybase, MySQL, and MongoDB), file systems, networks, and storage architecture.

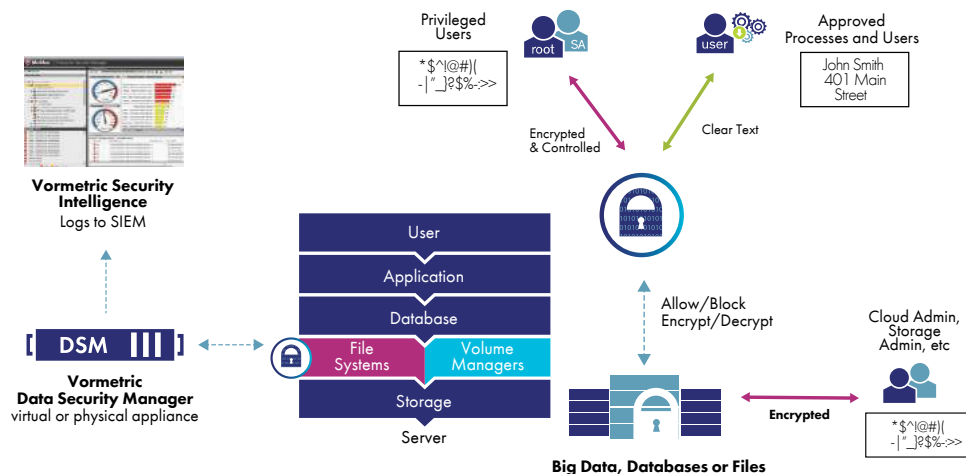


Figure 4: Vormetric Transparent Encryption enforcing least privilege policies to privileged users

User access control policies address system and LDAP/Active Directory roles as well as Hadoop users for big data environments.

The solution also provides security intelligence through its extensive auditing capabilities. Included are pre-built integrations and dashboards for popular SIEM tools such as Splunk, HP Arcsight, IBM QRadar and others.

When the Vormetric Live Data Transformation capability is also enabled with an additional license, encryption and rekeying of data can be performed without taking applications offline.

Vormetric Container Security

Extends Vormetric Transparent Encryption encryption, access controls and data access audit logging to data stored within, or accessed from, container environments.

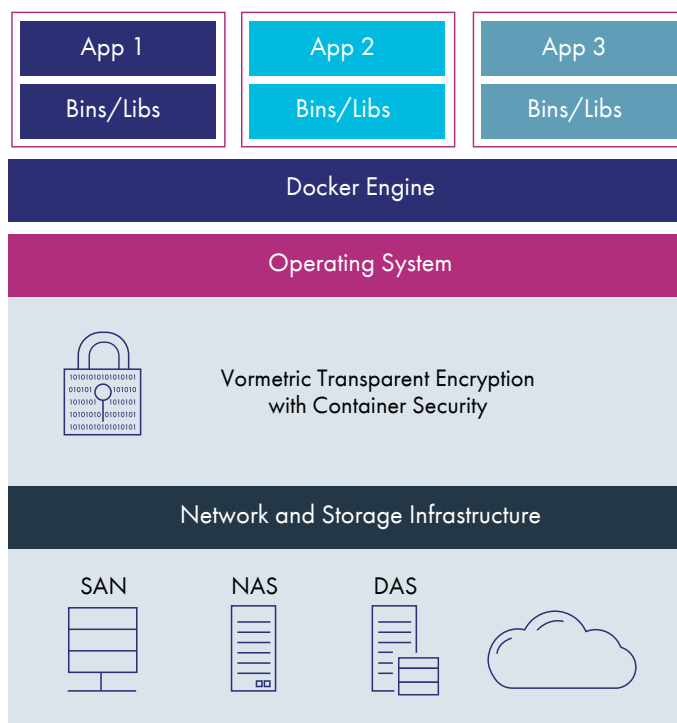


Figure 5: Vormetric Transparent Encryption with Vormetric Container Security

Vormetric Application Encryption

Vormetric Application Encryption, encrypts specific files or columns in databases, big data nodes, and platform-as-a-service (PaaS) environments. The application encryption solution features a set of documented, standards-based APIs that can be used to perform cryptographic and key management operations - eliminating the time, complexity, and risk of developing and implementing an in-house encryption and key management solution.

Access controls to data encrypted with the solution are under the control of the application developer or application administrator, dependent upon the architecture of the application.

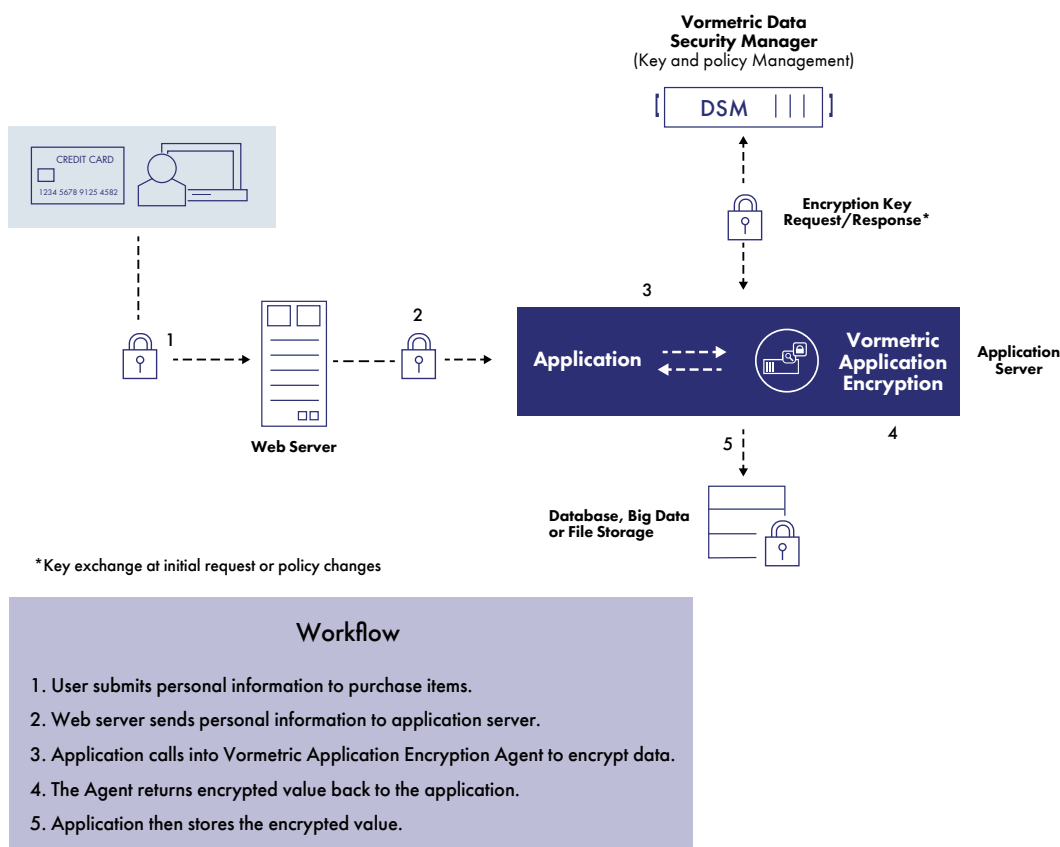


Figure 7: Vormetric Application Encryption Operation

Vormetric Tokenization with Dynamic Data Masking

Vormetric Vaultless Tokenization with Dynamic Data Masking dramatically reduces the cost and effort required to comply with security policies and regulatory mandates. The solution delivers capabilities for database tokenization and dynamic display security. The solution allows healthcare enterprises to efficiently address objectives for securing and anonymizing sensitive assets—whether they reside in data center, big data, container or cloud environments.

Dynamic data masking capabilities enable administrators to establish policies to return an entire field tokenized or dynamically mask parts of a field. For example, a security team could establish policies so that a user with customer service representative credentials would only receive a Social Security number with the last four digits visible, while a customer service supervisor could access the full number.

Conclusion

As HIPAA is no longer a “paper tiger,” covered entities and business associates must now verify that those they choose to do business with are following the rules. Thanks to tools provided by Thales, adherence to those critical compliance controls has become easier. Thales eSecurity allows organizations to meet their HIPAA compliance obligations in a timely, cost-effective manner with little administrative overhead, protecting sensitive patient information while still allowing organizations to meet both their data security and business objectives.

About Thales

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.

Decisive technology for decisive moments.

1 <https://dtr.thalesecurity.com/#hccpopup>

2 45 CFR 164.308(a)(1)(ii)(A).

3 <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf>

4 US Department of Health and Human Services, Federal Register 19006, 4/27/09, <https://www.federalregister.gov/documents/2009/04/27/E9-9512/guidance-specifying-the-technologies-and-methodologies-that-render-protected-health-information>

5 www.hipaa.com/2009/09/hipaa-protected-health-information-what-does-phi-include

THALES

Americas

Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA

Tel: +1 888 343 5773 or +1 512 257 3900

Fax: +1 954 888 6211 | E-mail: sales@thalessec.com

Asia Pacific – Thales Transport & Security (HK) Ltd

Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633

Fax: +852 2815 8141 | E-mail: asia.sales@thales-esecurity.com

Europe, Middle East, Africa

350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF

Tel: +44 (0) 1844 201800 | Fax: +44 (0) 1844 208550

E-mail: emea.sales@thales-esecurity.com

> thalesgroup.com <



Copyright © 2020 Fortrex. All rights reserved. Fortrex is a registered trademark of Fortrex Technologies. All other trademarks are the property of their respective owners.
No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, photocopying, recording or otherwise, without prior written consent of Fortrex.