A Fortrex White Paper

Using Encryption and Access Control for HIPAA Compliance
**Introduction**

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 found in HIPAA and HITECH. More than ever before, organizations have a heightened sense of responsibility and awareness to focus on securing their data. One of the most current topics being explored is encryption of data, followed by increased exercise of access control, logging and monitoring.

Prompting these investigations is an organization’s security risk analysis, which is a requirement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Security and Breach Notification Rules. As part of its comprehensive risk analysis, the organization must address whether encryption of data at rest, as an addressable implementation specification, (45 CFR 164.312 (a)(2)(iv)), is reasonable, appropriate, and cost effective. 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.

This paper has been prepared to present the complementary features of the Vormetric Data Security Platform to secure Personal Healthcare Information (PHI) data in accordance with the HIPAA implementation requirements.

Fortrex’s evaluation of the Vormetric Data Security Platform and its various security capabilities has revealed that Vormetric’s platform is capable of supporting an organization’s goals for achieving the encryption, access control, logging and monitoring technical requirements of HIPAA. Every organization is unique in its implementation of the administrative, technical, and physical security requirements of HIPAA. As such, carefully review the recommendations in this paper within the context of your existing or prospective environment. While this paper does not provide detailed instructions for how to configure Vormetric products within your environment, it provides the reader with product information and a roadmap for compliance to specific HIPAA regulations.

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 of privacy and security from the healthcare industry. Virtualization and cloud computing can create additional challenges in achieving compliance with HIPAA and HITECH, but does not inherently prevent compliance.
HIPAA/HITECH/Omnibus Rule Summary

This paper assumes the reader is familiar with HIPAA/HITECH (including relevant guidance publications).

The regulation of protected health information began in 1996 with the passage of the Health Insurance Portability and Accountability Act of 1996, commonly referred to as HIPAA. Although the regulation envisioned robust protections, the regulatory requirements arguably outpaced the technological capabilities of many organizations at the time. Compliance lagged, as organizations struggled with requirements that were in dire need of clarification and technologies that could not address all of the mandates in the law.

In 2009, however, a companion bill was passed that sought to clarify and tighten some of the requirements contained in HIPAA. The Health Information Technology for Economic and Clinical Health Act, or HITECH, provided a much needed update to HIPAA. Creating breach notification laws and a de facto requirement for encryption, the law sought to encourage the adoption of health information technology and to ensure the organizations handling or processing that data were taking appropriate steps to protect that data.

HIPAA/HITECH applies to all organizations that store, process, or transmit Protected Healthcare Information (PHI). Under the recent Omnibus Rule, this includes merchants, service providers, payment gateways, data centers, and outsourced service providers.

Although this paper specifically addresses HIPAA/HITECH compliance, the similar principles can be applied when implementing systems that comply with other privacy and security regulations, such as the Gramm-Leach-Bliley Act (GLBA), Sarbanes Oxley (SOX), Payment Card Industry (PCI), the Federal Information Security Management Act (FISMA) and so on.

On Jan. 25, 2013, a set of final regulations, referred to as “HIPAA Omnibus Rule”, was published by the Department of Health and Human Services (HHS) to modify the HIPAA Privacy, Security, and Enforcement Rules to implement various provisions of the HITECH Act. This Omnibus Rule makes it necessary for business associates to comply with the HIPAA Security Rule and most provisions of the HIPAA Privacy Rule, and they are now directly liable for enforcement action and fines imposed by the U.S. Department of Health and Human Services (HHS). Business associates may also be selected for an audit by the Office of Civil Rights.

Despite the clarifications contained in the HIPAA Omnibus Rule, many organizations still struggle to define their obligations under the law and to determine how to comply while maintaining fiscal responsibility and IT performance objectives. This paper offers some clarification on the requirements of HIPAA/HITECH with respect to the implementation of the Vormetric data protection platform for the protection of PHI.

HIPAA/HITECH Requirements

HIPAA is comprised of a set of rules that address the privacy, security, technical, administrative, organizational, and policy and procedure controls and implementation specifications related to PHI. The HITECH Act and Omnibus Rule enhanced enforcement of these rules. While all of these regulations have a variety of requirements, this paper focuses on the relevant portions of the legislation addressed by the Vormetric Data Security Platform.

The HIPAA Security Rule implementation specifications are divided between "required" and "addressable" components. While "required" clearly requires the organization to fully implement the particular specification, what "addressable" means has been misinterpreted. The Department of Health and Human Services has provided guidance for "addressable" specifications in its "HIPAA Administrative Simplification Regulation Text", March 2013: 2 "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." 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 risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI (ePHI). Managing these risks and ensuring that the proper security controls are in place are part of a good risk analysis, which is 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 that data 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, HIPAA suggests that companies implement encryption and decryption procedures. At the time the law was under consideration, these technologies were considered to be addressable specifications. Combined with the requirement to perform a risk analysis, and implement controls deemed reasonable and appropriate, it is easy to see how the growth in technology was considered in the early writing of the rules. Specifically, the Security Rule required the following technical safeguards:

<table>
<thead>
<tr>
<th>Category</th>
<th>Technology</th>
<th>Required or Addressable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Controls</td>
<td>Unique User ID</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Emergency Access Procedures</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>Automatic Log-off</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td>Encryption and Decryption</td>
<td>Addressable</td>
</tr>
<tr>
<td>Audit Controls</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>Authenticate Electronic PHI</td>
<td>Required</td>
</tr>
<tr>
<td>Person or Entity Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmissions Security</td>
<td>Integrity Controls</td>
<td>Addressable</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>Addressable</td>
</tr>
</tbody>
</table>

Note that many of the requirements that were deemed “addressable” at the time, but were categorized that way because the technology was expensive, complex, or not widely available. The HIPAA Security Rule was scalable and allowed for companies to conduct a risk assessment to see if the requirement could be met with an alternative solution. Today, many of those “addressable” requirements, particularly encryption, are proven, widely available and provide more manageable protection than was the case in the late 1990s.
Covered Entities and Business Associates - The Omnibus Rule

On January 17, 2013, HHS announced changes to HIPAA to strengthen the required privacy and security protections for PHI. The Omnibus Rule expanded many of the requirements to business associates that create, receive, maintain, or transmit PHI, such as contractors and subcontractors. Some of the largest breaches reported to HHS have involved business associates. Penalties for a breach of PHI were substantially increased based on the level of negligence, with a maximum penalty of $1.5 million per violation. The changes also affected the HITECH Breach Notification requirements by clarifying when breaches of unsecured PHI must be reported to HHS. The Omnibus Rule went into effect on March 23, 2013, and compliance with the law was required as of September 23, 2013.

HITECH Enforcement Provisions

For several years after the adoption of HIPAA, enforcement of the law was minimal. 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).

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Violations of Identical Provisions in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did not know</td>
<td>$100 – $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 – $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – Corrected</td>
<td>$10,000 – $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

The HHS OCR is responsible for enforcing compliance with the Security and Privacy Rules among covered entities. The FTC issued the Health Breach Notification Rule on February 22, 2010 to require certain business not covered by HIPAA to notify customers when a breach of individually identifiable electronic health information has occurred. This rule enforces compliance among vendors or personal health records (PHRs), PHR-related entities, and third party service providers to PHRs.

It is worth noting that HHS settled a case with a firm for $150,000 in December 2013 where it had identified that policies and procedures were needed to address breach notification provisions with HITECH.
Overview of the Vormetric Data Security Platform

Vormetric puts control in the health care administrator’s hands by encrypting ePHI and controlling 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: Vormetric Data Security Platform
Data Security Manager

The Vormetric Data Security Manager integrates key management, data security policy management, and audit log collection. This enables data security administrators to easily manage standards-based encryption across Linux, UNIX, and Windows operating systems in both centralized and geographically distributed physical, virtual and cloud environments. Clustering DSMs provides high availability and scalability to tens-of-thousands of protected servers.

![Figure 2: Controlling and Securing PII/PHI Data in the Cloud and On Premise](image)

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 premise or in the cloud. Either deployment model can be used for compliance to the HIPAA/HITECH requirements. It’s 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-premise or in the cloud
- As a service through AWS Marketplace.
Vormetric Transparent Encryption

Vormetric Transparent Encryption (VTE) 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 3: Vormetric enforcing least privilege policies to privileged users

Vormetric also provides security intelligence through its extensive auditing capabilities. These logs can be integrated with popular SIEM tools such as Splunk, HP Arcsight, IBM QRadar and others.
How Vormetric Contributes to HIPAA Compliance

HIPAA states that organizations should protect ePHI through the implementation of encryption. Typically, various solutions are deployed to provide protection for different applications, data types and infrastructures – this 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 number that are in databases, can be readily located and protected, unstructured data frequently found in EMR’s, medical images and other files dispersed across multiple environments can be more difficult to identify and protect. An additional challenge lies in controlling access to ePHI, as IT administrators with no-need-to-know about the data have full access. The best way to meet these requirements is through data at rest encryption, access control and audit logs.

Vormetric Data Security addresses the requirements in the HIPAA Security Rule while avoiding re-coding applications or cumbersome integration. Vormetric Data Security protects ePHI by encrypting the information and controlling access to the data. Using policy-based encryption, Vormetric ensures that only authorized users and services can encrypt and decrypt the data.

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 “unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute”.

Vormetric Data Security also overcomes the challenge of securing heterogeneous data types. Many encryption solutions provide protection only for structured data – those that can be found in databases or in other easily identifiable data stores. The very definition of ePHI renders many of those solutions moot. PHI 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.” This definition could include a vast array of different file types (audio files, graphic files, movies, etc) that reside in varying locations across a widely dispersed network environment. Perhaps most importantly, encrypting ePHI offers a safe harbor in the event of a compromise. If the network or system that stores ePHI is compromised, companies that have rendered the ePHI unreadable, as per the HIPAA statute, are exempt from the notification requirements of HITECH.

Restricting Access to ePHI

Vormetric Data Security enables compliance with HIPAA/HITECH access control requirements by offering organizations the ability to layer additional access control functionality beyond the native file system. Vormetric’s access controls follow the least-privilege model, which denies any activity that has not been expressly permitted. Vormetric’s access control capabilities allow authorized system level users to perform their intended functions while taking the ability to view clear-text away from these SysAdmins. The meta-data remains in clear text so SysAdmins still have the ability to manage the files as needed.

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. Proving compliance to auditors is easy with Vormetric’s standards-based syslogs that capture successful and failed user and application data access with granular details. 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 (APT), or the presence of a hacker attempting to access data.
Vormetric Controls and Support Matrix

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

Table 1: Applicability of HIPAA/HITECH Controls to Vormetric Security Platform

<table>
<thead>
<tr>
<th>REQUIREMENT DESCRIPTION</th>
<th>VORMETRIC CAPABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Risk Management:</strong> 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.</td>
<td>The Vormetric Data Security Platform provides detailed security intelligence on who, what, when and how data was accessed. Vormetric provides logging of access at the File Systems level. All read/write requests to sensitive data are tracked with security 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 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.</td>
</tr>
</tbody>
</table>

| 164.308(a)(1)(ii) | • Risk Analysis  
• Risk Management |

<table>
<thead>
<tr>
<th>REQUIREMENT DESCRIPTION</th>
<th>VORMETRIC CAPABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Management:</strong> 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 &quot;unknown” to the “known” in a technical environment.</td>
<td>Encryption and 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, Vormetric creates a management environment with strong separation of duties. 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 Data Security Platform.</td>
</tr>
</tbody>
</table>
Vormetric’s 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.

Vormetric supports Access Management by adding a layer of access control on top of the native operating system access control. 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 data. The solution enables least privilege access without interfering with normal administrative operations.

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

Vormetric not only generates audit information for unintended direct access to ePHI/PII data, 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 data under its control.

### REGULATION REFERENCE

<table>
<thead>
<tr>
<th>REGULATION</th>
<th>REQUIREMENT DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308 (a)(4)(ii)(B,C)</td>
<td>• Access Authorization and, Establishment, and Modification</td>
</tr>
<tr>
<td>164.308 (a)(5)(ii)(C)</td>
<td>• Login Monitoring</td>
</tr>
<tr>
<td>164.312 (a)(2)(i)</td>
<td>• Unique User ID</td>
</tr>
<tr>
<td>164.312 (a)(2)(ii)</td>
<td>• Emergency Access Procedure</td>
</tr>
<tr>
<td>164.312(a)(2)(iii)</td>
<td>• Automatic Logoff</td>
</tr>
<tr>
<td>164.312(c)(1,2)</td>
<td>• Integrity and authenticity of ePHI</td>
</tr>
</tbody>
</table>

### 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.

### VORMETRIC CAPABILITIES

Vormetric supports file level and volume level encryption that expands encryption beyond a single file or a database column. Vormetric 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. Vormetric performs the encryption/decryption functions, as opposed to granting authorized and authenticated users access to the key. See the following requirement for Key Management.
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.

VORMETRIC CAPABILITIES

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

Vormetric ensures cryptographic keys are centrally generated and stored by the Data Security Manager. The actual keys are never visible to anyone, including key custodians or systems administrators.

Vormetric restricts access to keys and key management activities by managing access within the Vormetric Data Security Manager, which decouples access rights from central access management systems such as Active Directory, thus restricting access by privileged users such as system administrators and root unless explicitly granted within Vormetric’s Data Security Manager.

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

• Cryptographic keys are centrally generated by the Data Security Manager 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 one-time-use AES 256 key and sent over a mutually authenticated TLS connection.

• Manual clear-text cryptographic key management is not required by Vormetric. Custodians can create keys, but key values are not visible to the custodian. 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 Data Security Manager 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 Data Security Manager archive into a new or replacement Data Security Manager.
Vormetric encrypts the data encryption keys with an AES 256-bit key. This encrypted key is stored securely on the Data Security Manager (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.

Vormetric also offers an option that stores the keys within a secure cryptographic device known as a host security module (HSM).

**REGULATION REFERENCE**

- 164.312 (a)(2)(iv)  
  - Encryption and Decryption
- 164.312 (e)(2)(i)  
  - 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

**VORMETRIC CAPABILITIES**

Vormetric 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.

Vormetric 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.

Vormetric generates audit information for unintended direct access to PHI/PII data and can be configured to generate alerts thus providing integrity monitoring for PHI/PII data under its control.

The DSM can be configured to synchronize with an NTP server for accuracy of date/time.

### REGULATION REFERENCE

| 164.312 (b) | • Audit Controls |

### REQUIREMENT DESCRIPTION

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

### VORMETRIC CAPABILITIES

Vormetric 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.

### VORMETRIC CAPABILITIES

Vormetric 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.
Although the Data Security Manager does not store the ePHI/PII data 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 Vormetric Data Security Manager 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.

While Vormetric does 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, Vormetric 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.
Vormetric 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.

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

The Vormetric solution has the ability to alert on critical events such as unauthorized access to ePHI/PII data 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.

<table>
<thead>
<tr>
<th>REGULATION REFERENCE</th>
<th>REQUIREMENT DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.310 (d)(1)</td>
<td>• Device and Media Controls</td>
</tr>
<tr>
<td><strong>VORMETRIC CAPABILITIES</strong></td>
<td>Security Reminders: Organizations should receive periodic security updates.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REGULATION REFERENCE</th>
<th>REQUIREMENT DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>164.308 (a)(5)(ii)(A)</td>
<td>• Security Reminders</td>
</tr>
</tbody>
</table>
Conclusion

With the passage of HITECH in 2009, the requirement to protect ePHI became much more than a “paper tiger,” as HIPAA has sometimes been described. Long on mandates and short on enforcement capability, HIPAA failed to drive compliance in the way that the regulators had envisioned. However, with the notification requirements and the enforcement provisions of HITECH, adoption has become a critical objective for covered entities and business associates. Despite the clear mandate from the regulators, however, compliance is still complex and can be burdensome. Vormetric Data Security, however, allows organizations to meet compliance 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 Vormetric

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Data is the new currency and Vormetric helps over 1300 customers, including 17 of the Fortune 25 and many of the world's most security conscious government organizations, to meet compliance requirements and protect what matters — their sensitive data — from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application — anywhere it resides — with a high performance, market-leading data security platform that incorporates application transparent encryption, privileged user access controls, automation and security intelligence. For more information, please visit: www.vormetric.com.

About Fortrex Technologies, Inc.

Founded in 1997 Fortrex Technologies, Inc. has been a market leader in providing IT Governance, Risk, and Compliance Advisory services and solutions to over 1,000 customers in various industry sectors.

Fortrex Technologies’ corporate mission is to be our clients’ long-term, trusted security and risk management advisor by ensuring the confidentiality, integrity, and availability of their data and systems through the provision of world-class, enterprise-wide information security services and solutions.

At Fortrex, we believe that our unique differentiator is the team of individuals who are committed to a set of corporate values. These values, Integrity, Excellence, Empowerment, Teamwork and Thankfulness, are the foundation of all Fortrex relationships, including those with our employees, customers and vendors.

References & Resources


3: US Department of Health and Human Services, “Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals” www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html