DATA SHEET

RACK FOUNDRY

Total Security Management HIPAA Compliance Guide

Be CYBERACTIVE

All organizations that store, process, or transmit Protected Health Information (PHI) need to meet the Health Insurance Portability and Accountability Act (HIPAA) compliance requirements to ensure the security of their electronic health information.

RackFoundry Total Security Management (TSM) helps to achieve and simplify HIPAA compliance. TSM not only enhances your network security but prepares you for the next audit by continually monitoring files that store sensitive patient data, detecting unauthorized changes to access controls, detecting vulnerable areas before they can be exploited, and providing HIPAA Compliance Reports as well as User Activity Reports.

RackFoundry TSM combines the essential security tools such as Security Information Event Management (SIEM), Centralized Logging, Intrusion Detection, Intrusion Prevention, File Integrity Monitoring, Asset Inventory, and Vulnerability Scanning along with our Security Operations Center services to provide continuous protection of your ePHI.

Our Security Operations Center is staffed 24/7/365 with RackFoundry Security Analysts that utilizes HIPAA best practices. The table below lists how RackFoundry TSM addresses and fulfills each requirement.

HIPAA Standard	HIPAA Requirement	Example of how RackFoundry TSM Helps
§ 164.306 Security standards: General rules.		
§ 164.306 (a) General requirements	Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.	RackFoundry TSM helps to ensure the confidentiality and integrity of electronic health information by continually monitoring inbound/outbound traffic (blocking threats by utilizing the built in Intrusion Prevention or Web Application Firewall), user activity, file changes (utilizing File Integrity Monitoring), and providing alerts for detected threats and hazards.
§ 164.308 Administrative safeguards.		
§ 164.308 (a) (1) (ii) (A) Risk analysis (Required)	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	RackFoundry TSM helps to ensure the confidentiality and integrity of electronic health information by continually monitoring inbound/outbound traffic (blocking threats by utilizing the built in Intrusion Prevention or Web Application Firewall), user activity, file changes (utilizing File Integrity Monitoring), and providing alerts for detected threats and hazards.
164.308 (a) (1) (ii) (D) Information system activity review (Required)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	RackFoundry TSM supports this requirement by gathering audit logs and providing alerts and reports for security incidents.

Continued to next page

Continued from previous page

HIPAA Standard	HIPAA Requirement	Example of how RackFoundry TSM Helps
164.308 (a) (5) (ii) (B) Protection from malicious software (Addressable)	Procedures for guarding against, detecting, and reporting malicious software.	RackFoundry TSM includes signature-based Network Intrusion Detection/Prevention as well as Host Intrusion Detection/Protection to detect and prevent malicious software from entering your environment infecting hosts. RackFoundry TSM's Vulnerability Scanner detects vulnerable areas before they are able to be exploited by malicious software.
164.308 (a) (5) (ii) (C) Log-in monitoring (Addressable)	Procedures for monitoring log-in attempts and reporting discrepancies.	Host Intrusion Detection (HIDS) agents monitor log-in attempts to your network devices and SIEM correlates failed log-in attempts, unauthorized log-ins, and more with other events to detect threats and generate alerts. RackFoundry TSM includes User Activity Reports that includes details about log-in attempts.
164.308 (a) (5) (ii) (D) Password management (Addressable)	Procedures for creating, changing, and safeguarding passwords.	RackFoundry TSM's Vulnerability Scanner detects weak passwords and File Integrity Monitoring (FIM) detects modifications to password files. RackFoundry's SIEM correlates all events to detect security threats.
164.308 (a) (6) (ii) Implementation specification: Response and reporting (Required)	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 or business associate; and document security incidents and their outcomes.	RackFoundry TSM helps users quickly identify and respond to security threats with continuous monitoring and actionable alerts. RackFoundry's Security Operations Center (SOC) helps customers mitigate security incidents.

Continued to next page

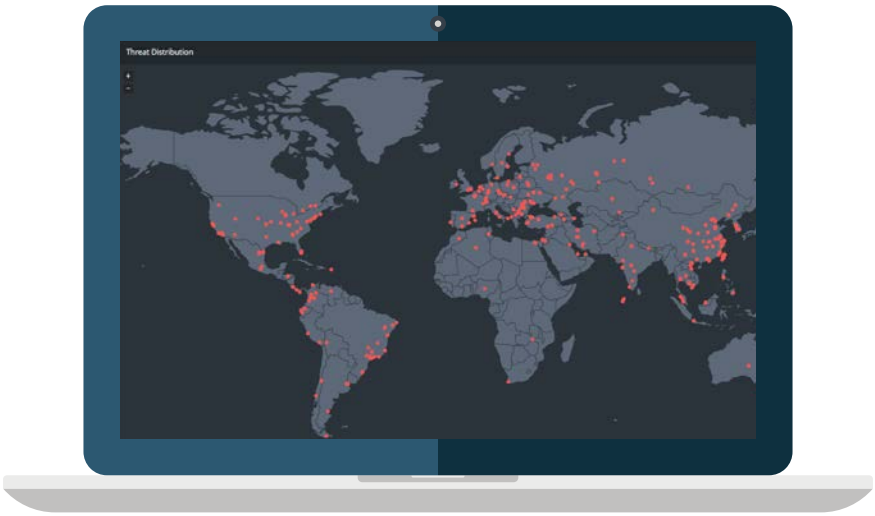
Continued from previous page

HIPAA Standard	HIPAA Requirement	Example of how RackFoundry TSM Helps
§ 164.310 Physical safeguards.		
§ 164.310 (d) (1) Standard: Device and media controls	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.	Host Intrusion Detection (HIDS) agents detect the removal of electronic media that contains electronic protected health information (such as USB drives). File Integrity Monitoring detects changes to files that contain ePHI. RackFoundry's SIEM correlates all events to detect security threats.
§ 164.312 Technical safeguards.		
§ 164.312 (a) (2) (i) Unique user identification (Required)	Assign a unique name and/or number for identifying and tracking user identity.	RackFoundry TSM monitors log-ons to detect user ID's that are being used by multiple users.
§ 164.312 (a) (2) (iv) Encryption and decryption (Addressable)	Implement a mechanism to encrypt and decrypt electronic protected health information.	RackFoundry TSM's VPN allows for remote access of ePHI. RackFoundry TSM detects when encryption/decryption procedures are not correctly utilized.
§ 164.312 (b) Standard: Audit controls	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	RackFoundry TSM monitors and archives logs and events related to devices that contain or use ePHI.
§ 164.312 (c) (1) Standard: Integrity	Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	RackFoundry TSM's File Integrity Monitoring (FIM) detects altercation and destruction to files containing ePHI.

Continued to next page

Continued from previous page

HIPAA Standard	HIPAA Requirement	Example of how RackFoundry TSM Helps
§ 164.312 (e) (2) (ii) Encryption (Addressable)	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	RackFoundry TSM's VPN allows for remote access of ePHI.



RackFoundry TSM leverages essential security capabilities to help organizations of all sizes achieve HIPAA compliance. In addition, RackFoundry's Security Operation Center ensures that security threats are addressed quickly and effectively 24/7/365.

About RackFoundry

RackFoundry, the maker of Total Security Management (TSM), is a leader in complete coverage security appliances, secure cloud services and professional services such as SecurityXpert that provides security expertise to organizations of all sizes and industries. The RackFoundry security team, FortressLabs™, help find new vulnerabilities in the wild, mitigate any found vulnerabilities, and head up the RackFoundry Security Operations Center.

For more information mus at www.rackfoundry.com.