



VMware® SDDC / EUC Product Applicability Guide for the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

Published March 2016
Updated October 2016

TECHNICAL WHITE PAPER

This is the first document in the compliance reference architecture for HIPAA/HITECH. You can find more information on the framework and download the additional documents from the HIPAA/HITECH compliance resources tab on VMware Solution Exchange [here](#).

Table of Contents

Executive Summary	5
Introduction	5
Scope and Approach	7
HIPAA Security Rule Scope	8
VMware Solution Scope	8
Our Approach	12
VMware and HIPAA Security Rule Requirements (Overview)	13
VMware Control Capabilities Detail (By HIPAA Security Rule)	17
Administrative Safeguards 164.308	17
Physical Safeguards 164.310	25
Technical Safeguards 164.312	27
Summary	32
Appendix A (HIPAA Security Rule)	33
Appendix B (What is Cloud)	33
Appendix C (Product Listing)	33
Glossary of Terms	33
Bibliography	33
Acknowledgements	34
About Coalfire	34

Revision History

DATE	REV	AUTHOR	COMMENTS	REVIEWERS
December 2015	0.1	Jason Macallister	Initially Created	Internal SME, Coalfire
March 2016	0.2	Jason Macallister	Revised per VMware SME Response	VMware Subject Matter Experts
March 2016	1.0	Jason Macallister	Final Document	
October 2016	1.1	VMware CCRS team	Updates to Final Document	

Design Subject Matter Experts

The following people provided key input into this design.

NAME	EMAIL ADDRESS	ROLE/Comments
Jason Macallister	jason.macallister@coalfire.com	Senior Consultant – Cloud and Virtualization
Andrew Hicks	andrew.hicks@coalfire.com	Senior Consultant – Healthcare Practice
Chris Krueger	chris.krueger@coalfire.com	Revision QA to Customer DRAFT Release
Anthony Dukes	adukes@vmware.com	Technology SME, VMware
Chris Davis	chrisdavis@vmware.com	Security and Compliance SME, VMware

Trademarks and Other Intellectual Property Notices

The VMware products and solutions discussed in this document are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their companies.

Solution Area	Key Products
Software-Defined Compute	VMware ESXi™, VMware vCenter™, VMware vCenter Server™, VMware vCloud Suite®
Software-Defined Networking	VMware NSX®, VMware NSX Edge™, NSX Firewall, NSX Router, NSX Load Balancer, NSX Service Composer
Management and Automation	VMware vRealize® Operations™, VMware vRealize® Operations Manager™, VMware vRealize® Hyperic®, VMware vRealize® Configuration Manager™, VMware vRealize® Infrastructure Navigator™, VMware vRealize® Log Insight™, VMware vRealize® Operations Insight™, VMware vRealize® Orchestrator™, VMware vRealize® Operations for Horizon®, VMware vRealize® Operations for Published Applications™, VMware vRealize® Operations Manager™ for Horizon®, VMware vRealize Automation™, VMware vRealize Business™
Disaster Recovery Automation	VMware vCenter™ Site Recovery Manager™
End User Computing	VMware Horizon®, VMware Horizon® View™ Standard Edition, VMware Horizon® Client, VMware Mirage™, VMware Workspace™ Suite, VMware Horizon® DaaS®, VMware Workspace™ ONE™
Enterprise Mobility Management	AirWatch® Mobile Device Management, AirWatch® Mobile Application Management, VMware AirWatch® Mobile Email Management, AirWatch® Content Locker, AirWatch® Mobile Browsing Management, AirWatch® Browser

Executive Summary

VMware recognizes the following as critical areas that must be addressed by each covered entity and business associate in the operation of healthcare information systems: security and compliance; the criticality and vulnerability of the assets needed to manage electronic protected health information (ePHI) impacting infrastructures; and the risks to which they are exposed. By standardizing an approach to compliance and expanding the approach to include partners, VMware provides its customers a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and auditors a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications to the cloud in a secure and compliant manner. This is especially important when the outcomes for noncompliance are extremely critical due to civil and criminal penalties imposed by the Office for Civil Rights (OCR) Department of Health and Human Services (HHS) and the U.S. Department of Justice (DOJ); not to mention, there is a high probability for collateral impact due to failure to protect patient privacy, institutional trust and economics. In extreme cases of breach or data loss, the fines and penalties are minor compared to the potential for litigation, recompense and/or public relations improvements.

For these reasons, VMware enlisted its audit partner, Coalfire Systems, to engage in a programmatic approach to evaluate VMware products and solutions for HIPAA Security Rule requirements capabilities and document these capabilities into a set of reference architecture documents. This document presents Coalfire's evaluation of the different VMware applications available to organizations that use (or are considering using) VMware software-defined data center (SDDC) and end-user computing EUC environments to host or access ePHI impacting critical cyber assets. Specifically, this document focuses on the SDDC and EUC solutions available. The software-defined data center is defined as a platform, which brings together best-in-class compute, storage, networking, security and technical management, virtualized and delivered as a service. A unified hybrid cloud lets you rapidly develop, automatically deliver, and manage all of your enterprise applications, no matter where they reside, from one, unified platform. To that end, Coalfire highlights the specific HIPAA Security Rule requirements that these applications address and/or support. The applications outlined in this product applicability guide can be considered in evaluation of the initial sourcing of technologies to build a platform which helps covered entities and business associates meet HIPAA requirements.

For more information on these documents and the general approach to compliance issues please review [VMware Compliance Cyber Risk Solutions](#).

The controls selected for this paper are from the HIPAA Security Rule published February 20, 2003. It has been reviewed and authored by our staff of cloud experts and HIPAA auditors in conjunction with VMware.

If you have any comments regarding this whitepaper, we welcome any feedback at vmware@coalfire.com or compliance-solutions@vmware.com.

Introduction

Most organizations begin the compliance process by mapping the mandated requirements to their specific organizational needs and capabilities. This is usually a difficult task that can utilize significant time and resources. To streamline the process, VMware has developed and established a single holistic approach that can be used to evaluate the VMware environment, partner solutions, and end user tools. This Product Applicability Guide, the first in a series of white papers that make up the reference architecture framework, maps HIPAA Security Rule requirements to VMware's software-defined data center and end-user computing technology platforms.

Organizations can significantly reduce the complexity and cost of HIPAA Security Rule compliance by replacing traditional non-integrated products with integrated solutions. As most organizations know, there is no single product or vendor that can meet all of an organization's needs. To further address this gap, VMware, together with the VMware partner ecosystem delivers compliance-oriented integrated solutions, enabling compliance by automating the deployment, provisioning and operation of regulated environments. VMware Compliance and Cyber Risk Solutions provide the solution reference architecture, HIPAA Security Rule specific guidance, and software solutions that businesses require to be able to achieve continuous compliance. VMware reference architecture framework combined with VMware hyper-converged solutions based on Intel architecture, enables IT to continually transform their data centers by speeding up Software Defined Infrastructures (SDI) and hybrid cloud deployments, enabling IT to advance innovation, optimizing system services in real-time, mobilizing workforce and customer interactions. These solutions improve security and control via secure compliance capable/audit



ready solutions, lower equipment and operational costs, and directly address agency needs for:

- Cost and infrastructure efficiency
- Simplified management and reporting
- Infrastructure transparency
- Effective Cyber Risk Management
- Ability to enable and maintain a secure and compliant environment

The VMware compliance reference architecture framework provides a programmatic approach to map VMware and partner products to regulatory controls, from an independent auditor perspective. The result is valuable guidance that incorporates best practices, design, configuration and deployment with independent auditor oversight and validation.

Figure 2 illustrates measures of capability with respect to security, confidentiality, and integrity that make up a trusted cloud implementation. The graphic illustrates the specific solution categories that can be addressed with VMware solutions and VMware's extensive partner ecosystem.

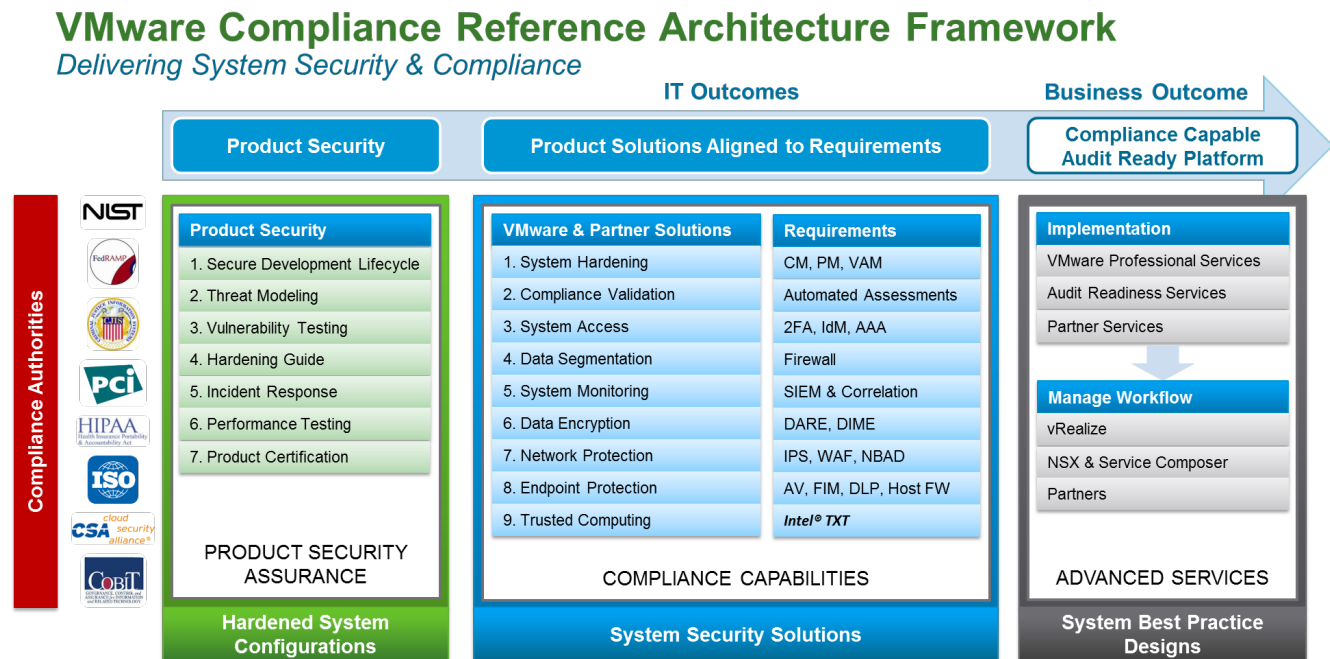


Figure 1: VMware Compliance Reference Architecture Framework

By addressing and implementing the security solutions within the framework of the regulated infrastructure many of the technical control requirements for any particular regulation are addressed. By integrating these security solution components together in a cohesive manner, the outcome is a compliance-capable, audit-ready platform upon which the covered entity or business associate can overlay its business systems and data.

Figure 2 further illustrates the alignment of system security solutions with compliance frameworks and gives examples of VMware technologies and solutions that are capable of addressing the solution.

Compliance Solutions Crosswalk - Common Required Technical Security Solutions

Common Required Technical Security Solutions

		HIPAA	FISMA MOD	PCI	NIST SP800-53A	HIPAA Security Rule	Product Examples
System Hardening & Compliance Validation							
1	Configuration Management	▲	●	●	SI-2, SA-10, CM-1/2/6, AC-7(2), AC-19	164.312c(1), 164.310(c)	VMware vRealize Configuration Manager, AirWatch Enterprise Mobility Management
2	Patch Management	▲	●	●	CM-2, SI-2	164.308(a)(5)(i)(B)	VMware vRealize Configuration Manager
3	Vulnerability Assessment and Management	●	●	●	RA-5, RA-3, SA-14	164.308(a)(1)(i)(A)/(B) 164.308(a)(8)	
4	Penetration Testing	▲	●	●	CA-2	164.308(a)(8)	
System Access							
5	Two Factor Authentication	▲	●	●	IA-2 (1), IA-4	164.312(d)	
6	Identity Management	●	●	●	IA-2, IA-4	164.308(a)(5)(i)(D) 164.312(a)(2)(i)	VMware Identity Manager
7	Access Management	▲	●	●	IA-5, AC-3	164.308(a)(4)(ii)(B)/(C) 164.308(a)(5)(ii)(c)	
Data Segmentation							
8	Network & Host Firewall	▲	●	●	SC-7	164.312(c)(2) 164.312(e)(2)(i)	VMware NSX Logical Firewall
System Monitoring							
9	Security Information Event Monitoring	●	●	●	SI-4, AU-2/3/6/10/12	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.312(b) 164.312(c)(2)	VMware vRealize Log Insight
10	Database Monitoring	■	▲	▲	SI-4		
Data Encryption & Protection							
11	Data At Rest Encryption	▲	●	●	SC-12/13/28, IA-7	164.312(a)(2)(iv) 164.312(c)(2)	
12	Data In Motion Encryption	▲	●	●	SC-9/12/13, IA-7	164.312(a)(2)(ii) 164.312(a)(2)(iv) 164.312(c)(1) 164.312(e)(2)(ii)	
13	System Backup & Restore	●	●	●	CP-9	164.308(a)(7)(iii)(A) - (E) 164.312(a)(1)	VMware Data Protection
Network Protection							
14	Intrusion Prevention System	■	●	●	SI-3, SI-4	164.312(c)(1) 164.312(e)(2)(i)	VMware NSX Platform Extensibility, vShield Endpoint
15	Web Application Firewall	■	▲	▲	SI-3, SI-4, SC-7	164.312(c)(1) 164.312(e)(2)(i)	VMware NSX Platform Extensibility, vShield Endpoint
Endpoint Protection							
16	Antivirus & Malware Prevention	▲	●	●	SI-3	164.308(a)(5)(i)(B)	VMware NSX Platform Extensibility, vShield Endpoint
17	File Integrity Monitoring	▲	●	●	SI-7	164.312(c)(2) 164.312(e)(2)(i)	
18	Data Leakage Protection	■	▲	▲	AC-4	164.312(e)(2)(i)	
Trusted Computing							
19	Trusted Execution	■	▲	▲		164.312(c)(1)	

Specifically discussed indicates that the technical security solution was specifically mentioned in a requirement

Not specifically discussed indicates that there was no specific mention of the solution; however, the solution may be inferred from the requirement

Possibly required indicates that the solution was specifically discussed, but is not considered a requirement. Typically this means that it is addressable if feasible.

Comments or suggestions: chrisdavis@vmware.com

● Specifically discussed

■ Not specifically discussed

▲ Possibly required (use case, risk, feasibility)

Figure 2: Compliance Solutions Crosswalk

Scope and Approach

Due to the HIPAA Security Rule's broad coverage of subjects relative to patient privacy, it is necessary to identify the subjects that are relevant to the combined subject matter of this product applicability guide. The primary subjects include the HIPAA Security Rule requirement topics and the VMware presented platform and solutions.

HIPAA Security Rule Scope

The compliance framework scope of this product applicability guide is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule (the Security Rule). To gain greater understanding of the requirements specified in the security rule, Coalfire refers to NIST Special Publication 800-66 Revision 1. Though NIST publications are primarily required for federal agencies, they are commonly used as voluntary guidelines and best practices for the private sector. The NIST publications are useful for assisting entities with selecting the type of implementation that best suits their unique circumstances. For each of the Security Rule requirements, Coalfire identified controls from NIST Special Publication 800-53 revision 4 that are in alignment. Using this foundation simplified the process for determining the capability of VMware solutions to address controls necessary to meet the requirement. For VMware technologies, the relevant HIPAA Security Rule requirements include:

164.308 Administrative Safeguards,

164.310 Physical Safeguards, and

164.312 Technical Safeguards

where the majority of relevant requirements are Technical Safeguards.

Reference architecture framework documents have been published by VMware for other compliance frameworks. If you are interested in learning more about VMware's approach to compliance with respect to additional regulatory frameworks, please review "VMware's Compliance & Cyber Risk Solutions" on the VMware Solution Exchange.

VMware Solution Scope

VMware provided a listing of VMware technologies to be included in scope for evaluation with regard to level of capability to support the HIPAA Security Rule requirements. Included in scope for this assessment are VMware's software-defined data center (SDDC) stack and the VMware end-user computing EUC stack. The SDDC stack is the foundation for enterprise virtualization and cloud platforms. The EUC stack utilizes the best of software-defined data center and enables improved management and control over the delivery of the end-user experience. These technologies when taken together form the basis for a cohesive infrastructure platform solution. The following is a listing of in-scope VMware technologies with a brief summary of each technology's purpose. More information about the technologies listed can be found at www.vmware.com.

Intel Trusted Execution Technology (Intel TXT) provides hardware-based security technologies to help build a solid foundation for security which enables IT to establish trusted pools of virtualized resources for stronger security and compliance in multi-tenant virtual and cloud environments. Built into Intel's silicon, these technologies address the increasing and evolving security threats across the virtual infrastructure. Intel TXT also can play a role in meeting government and industry regulations and data protection standards by providing a hardware-based method of verification useful in compliance efforts.

Intel Advanced Encryption Standard New Instructions (Intel AES-NI) accelerates the most compute-intensive steps of AES algorithms to significantly reduce the performance penalties of encryption. Supported in the VMware ESXi kernel, AES-NI accelerates encryption allowing you to encrypt / decrypt sensitive data and communications throughout your data center without the performance penalty of security.

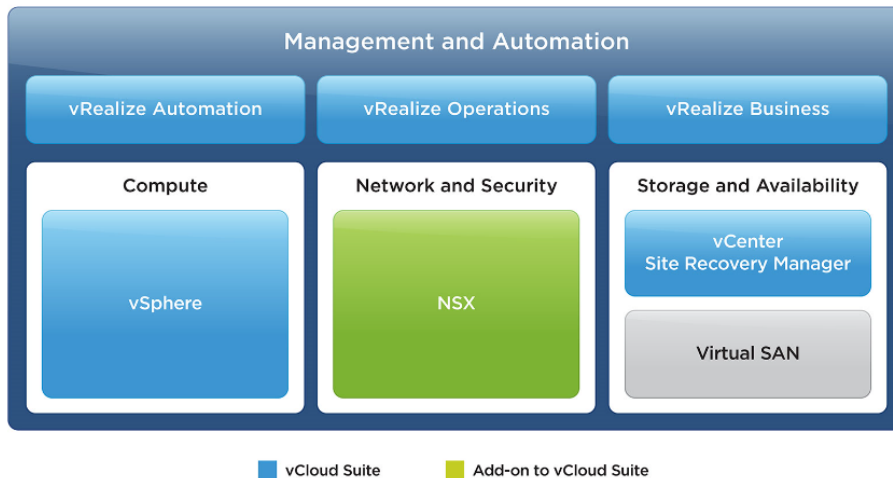
VMware vCloud Suite - Enterprise

The following is a listing of the individual products and features available with the VMware vCloud Suite – Enterprise. The VMware vCloud Suite is the base suite of products that make up the VMware software-defined data center.



vCloud Suite

Build and Manage a vSphere-Based Private Cloud



Note: Cloud management platform components of vCloud Suite, including vRealize Automation, Operations, and Business, are specifically designed for use with vSphere environments. vCloud Suite can be extended to hybrid cloud with vRealize Suite.

Figure 3: vCloud Suite

VMware vSphere

VMware vSphere is the leading server virtualization platform with consistent management for virtual data centers. It is the core foundational building block of highly virtualized environments and cloud infrastructure also referred to as the software-defined data center. The features listed below are relevant to HIPAA Security Rule requirements. They provide capabilities that are pertinent to the Security Rule including a secure platform architecture, management ease with integration for single pane of glass management, high availability, antivirus and antimalware support, and configuration awareness and consistency.

- VMware vSphere Hypervisor Architecture – a type 1 hypervisor
- VMware vSphere Storage APIs
- VMware vSphere High Availability
- VMware vSphere Fault Tolerance
- VMware vSphere Data Protection
- VMware vShield Endpoint
- VMware vSphere Reliable Memory
- VMware vSphere Distributed Switch
- VMware vSphere Auto Deploy
- VMware vSphere Host Profiles

VMware vCenter Server

VMware vCenter Server provides a centralized and extensible platform for management of vSphere virtual infrastructure. IT administrators can help ensure security and availability, simplify day-to-day tasks, and reduce complexity of managing a virtual infrastructure.

VMware Site Recovery Manager

VMware Site Recovery Manager is leading solution to enable application availability and mobility across sites in private cloud environments. It is the basis for fast and reliable IT disaster recovery. VMware Site Recovery Manager is an available extension to VMware vCenter, providing centralized management capability for disaster recovery, site migration and non-disruptive testing capabilities to VMware customers. Site Recovery Manager is fully integrated with VMware vCenter Server and VMware vSphere Web Client. It works in conjunction with various replication solutions including VMware vSphere Replication to automate the process of migrating, recovering, testing, re-protecting and failing back virtual machine workloads.

VMware vSphere Replication

VMware vSphere Replication is a hypervisor-based, asynchronous replication solution for vSphere virtual machines. It is fully integrated with VMware vCenter Server and the vSphere Web Client. VMware vSphere Replication delivers flexible, reliable and cost-efficient replication to enable data protection and disaster recovery for all virtual machines in the infrastructure. Combined with VMware Site Recovery Manager, VMware vSphere Replication is capable of addressing HIPAA requirements for emergency availability and to aid covered entities and business associates with business continuity.

VMware vRealize Business for vSphere

VMware vRealize Business provides transparency and control over the cost and quality of IT services, enabling the Chief Information Officer (CIO) to align IT with the business and to accelerate IT transformation. Understanding Return on Investment (ROI) and Total Cost of Ownership (TCO) helps to quickly identify ways to reduce costs while improving delivery of services to more directly support the business' objectives. Common in many of the HIPAA Security Rule addressable requirements is a notion of feasibility, that is, many of the addressable security rules, when applied to specific use cases, are aimed at improving the security posture of the covered entity and business associate. Understanding the costs to secure the environment should be useful in determining the feasibility of implementing a particular solution or features.

VMware vRealize Automation – Enterprise

VMware vRealize Automation improves agility by automating IT service delivery (applications, infrastructure, desktops and any IT service to rapidly respond to business needs). It allows for improved control of the IT solutions by enabling personalized, business-relevant policies to enforce application deployment standards, setting resource quotas and enabling multiple service levels. VMware vRealize Automation allows for improvements in efficiency by improving IT delivery while lowering cost. With automation, IT is able to offer the business self-service deployment capabilities without sacrificing control, and thus can ensure that necessary security controls are automatically applied to all newly deployed solutions. It further allows control for the covered entity beyond the private cloud with extensibility to multi-vendor, multi-cloud designs.

VMware vRealize Operations – Enterprise

Part of the vRealize vCloud Suite, vRealize Operations provides intelligent operations management capability for the covered entity's and business associate's physical, virtual and cloud infrastructure. It correlates data from applications to storage in a unified, easy-to-use management tool that provides control over performance, capacity and configuration, with predictive analytics to drive proactive action and policy-based automation. A challenge that faces any organization desiring to determine risk is the lack of knowledge and insight into the infrastructure. The VMware vRealize product family includes:

- VMware vRealize Operations Manager
- VMware vRealize Hyperic
- VMware vRealize Configuration Manager
- VMware vRealize Infrastructure Navigator
- VMware vRealize Log Insight
- VMware vRealize Operations Insight
- VMware vRealize Orchestrator



VMware NSX

VMware NSX is the network virtualization platform for the software-defined data center. By bringing the operations model of a virtual machine to your data center network, you can transform the economics of network and security operations. NSX lets you treat your physical network as a pool of transport capacity, with network and security services attached to virtual machines with a policy-driven approach.



Figure 4: VMware NSX Platform for Advanced Networking and Security Services

Networking for the software-defined data center

Agility and Streamlined Operations

Security and Micro-segmentation

Platform for advanced networking and security services

- Logical Switching
- NSX Gateway
- Logical Routing
- Logical Firewall
- Logical Load Balancer
- Logical VPN
- NSX API

VMware Workspace ONE

VMware End-User computing products allow IT organizations to pro-actively deliver consistent and intuitive services to their customers. Driven by the demands of users for immediate access to applications and data from any device, at any time, and from any place, services can be orchestrated to meet these demands without sacrificing compliance requirements. As a result, the user is able to work more efficiently in a manner that best suits his or her needs, while IT is able to manage that experience to ensure confidentiality, integrity and availability. VMware Workspace ONE combines end-user computing technologies from VMware and AirWatch by VMware to unify the end-user experience for secure access to applications and content from laptops, desktops, zero or thin-clients, and mobile devices and tablets.



Figure 5: VMware End User Computing

VMware Horizon 6 Enterprise Edition

- vSphere Desktop and vCenter Desktop
- Horizon with View
- Horizon for Linux
- vSphere and vCenter for Desktop
- vRealize Orchestrator + Desktop Plugin
- vRealize Operations for Horizon
- User Environment Manager
- Mirage
- App Volumes
- ThinApp

AirWatch Enterprise Mobility Manager

VMware AirWatch is a scalable enterprise mobility management platform that integrates with existing enterprise systems and allows you to manage all devices, regardless of type, platform or ownership, from one central console. Included with AirWatch Enterprise Mobility Manager are the tools necessary to allow end users, regardless of their device, to securely interact with HIPAA compliant workloads. The ability for administrators to manage and control the device ensures the integrity of the device and security of the data that these devices are accessing.

- AirWatch Container Management
- AirWatch Mobile Device Management
- VMware AirWatch Mobile Applications Management
- AirWatch Mobile Content Management
- VMware AirWatch Mobile Email Management
- AirWatch Mobile Browsing Management

VMware Identity Manager

VMware Identity Manager is an Identity as a Service (IDaaS) offering, providing application provisioning, self-service catalog, conditional access controls and Single Sign-On (SSO) for SaaS, web, cloud and native mobile applications. Identity Manager delivers on consumer-grade expectations like one-touch access to apps. This delivery of applications can be optimized with AirWatch Conditional Access and backed by a self-service catalog with enterprise-class management and security.

VMware Horizon FLEX

VMware Horizon FLEX provides the flexibility IT needs to serve BYO users, Mac users, contractors and road warriors while ensuring security, control and compliance for the corporate desktop. Horizon FLEX containerizes corporate windows desktops that are then distributed to these various devices. This containerization of the desktop allows for IT to implement all of the security measures required by the organization and to confirm that these measures are properly securing the workload and any data contained therein.

Our Approach

The HIPAA Security Rule Solutions Applicability Matrix, found in the sections following this document, maps specific requirements of the HIPAA Security Rule to VMware's solutions suites, their component technologies, and partner technologies where specifically integrated with made use of by the VMware technologies.

The understanding of the HIPAA Security Rule requirements is supported by NIST SP 800-66 and NIST 800-53 revision 4. Based on available product documentation, a notional determination of capabilities with respect to the requirement allowed



for the alignment process to determine the extent of attainability of the technology or the solution as a whole to address the HIPAA requirement. The inferences drawn upon by this common understanding support cases where the technology is specifically capable of attaining control enablement, the technology partially supports control enablement, and/or the technology does not undermine the requirement. Though HIPAA does not specifically include guidance relative to cloud and virtualization, the concepts of controls relative to confidentiality, integrity and availability are applicable to the software-defined data center.

Figure 6 illustrates the VMware's complete approach to compliance.

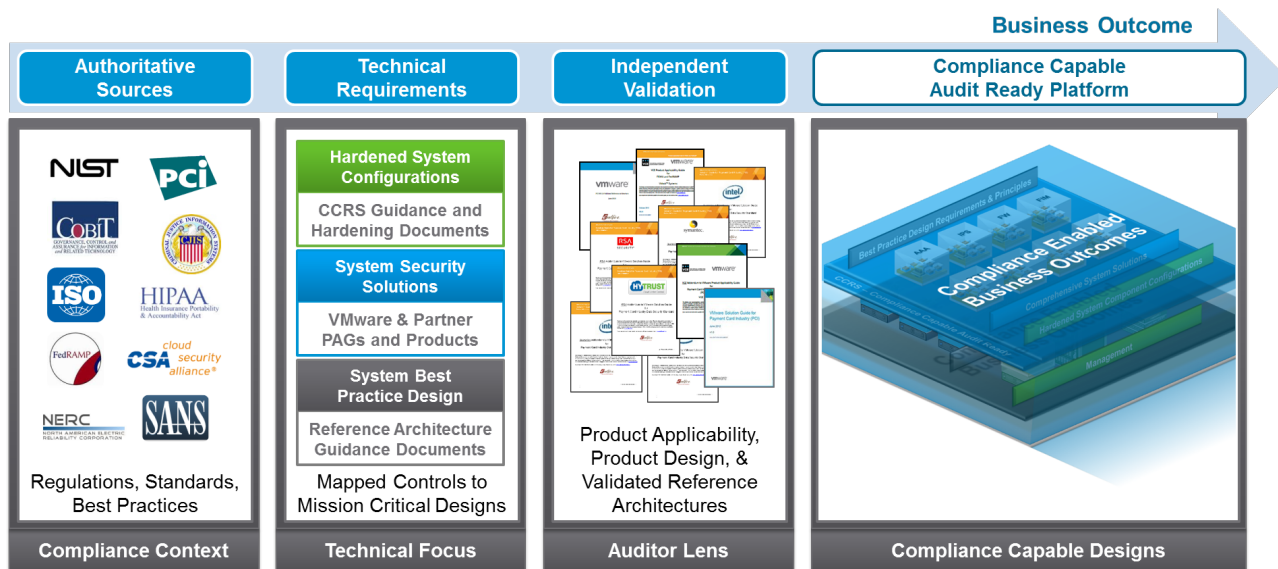


Figure 6: VMware's Compliance Reference Architecture Framework

VMware and HIPAA Security Rule Requirements (Overview)

VMware has created a HIPAA Security Rule requirement matrix to assist covered entities with understanding how VMware technologies align with and support the HIPAA Security Rule, both required and addressable standards. The requirement matrix presents Coalfire's assessment of the degree of compliance attainability for which VMware platform and platform management technologies combined with partner technologies can provide. The remaining standards are required or addressable by covered entities and business associates tools, policies, procedures, and training. While every cloud is unique VMware believes that a majority of technical standards can be addressed by VMware and Partner solutions.

HIPAA SECURITY RULE SAFEGUARDS		PRODUCTS
164.308	Administrative Safeguards	VMware vRealize Configuration Manager, VMware vRealize Log Insight, VMware vRealize Automation, VMware vSphere ESXi, VMware vCenter Server, VMware NSX, AirWatch Mobile Device Manager, VMware Identity Manager
164.310	Physical Safeguards	VMware ESXi, VMware vCenter Server, VMware NSX, VMware Workspace Suite, VMware User Environment Manager, VMware NSX for vSphere Horizon Edition, AirWatch Enterprise Mobility Management, vSphere Data Protection

HIPAA SECURITY RULE SAFEGUARDS		PRODUCTS
164.312	Technical Safeguards	VMware ESXi, VMware vCenter Server, VMware NSX, VMware vRealize Log Insight, VMware vRealize Configuration Manager, VMware vRealize Site Recovery Manager, VMware vRealize Workspace Suite, VMware User Environment Manager, VMware NSX for vSphere Horizon Edition, AirWatch Enterprise Mobility Management, VMware Identity Manager
164.314	Organizational Requirements	No VMware technologies applicable to these safeguards
164.316	Policies and Procedures and Documentation Requirements	No VMware technologies applicable; however, the covered entity or business associate can choose to reference VMware documentation as part of its required documentation.

Table 1: VMware Solutions Applicability to HIPAA Security Rule Safeguards

For a high level view, Table 1 matches up VMware technology capabilities to fully or partially support or address standards found in the HIPAA Security Rule safeguards.

Table 2 breaks out the HIPAA Standards under each of the HIPAA Security Rule Safeguards. The table summarizes the HIPAA Standards that are applicable to VMware technologies. Where the standard is primarily administrative or organizational in scope, the VMware technologies are determined to not be applicable to address the standard; however, there are cases where the assessor determined that it may be possible for the technology to support some of the activities associated with administrative or organizational standards. In this case the column will reflect that at least one VMware Technology or feature is capable of providing value for that standard. Applicability to VMware technologies and solutions indicates that the standard can be either fully or partially addressed by one or more of the technologies, features or the solution as a whole. Further detail will be provided in the following sections. In some cases the technology is capable of partially addressing the control requirements, in this case VMware partner solutions can be integrated to provide greater coverage of capability; notwithstanding, it is likely that managerial, organization or administrative procedures and training will be required to fully implement each standard.

Not Applicable – Indicates that VMware Technology is not applicable to the standard or implementation requirements.

Supports – Indicates that the standard or implementation is largely organizational and administrative in nature; however, VMware technology is capable of supporting the implementation.

Applicable – Indicates that VMware technology is capable of either fully or partially addressing the standard and implementation requirements.

REQUIREMENT ID	IMPLEMENTATION TOPIC	HIPAA STANDARD	APPLICABILITY TO VMWARE TECHNOLOGIES
164.308	Administrative Safeguards		
164.308 (a)(1)(i)	Security Management Process		Not Applicable
164.308 (a)(1)(ii)(A)	Risk Analysis	Security Management Process	Supports
164.308 (a)(1)(ii)(B)	Risk Management	Security Management Process	Supports
164.308 (a)(1)(ii)(C)	Sanction Policy	Security Management Process	Not Applicable
164.308 (a)(1)(ii)(D)	Information System Activity Review	Security Management Process	Supports
164.308 (a)(2)	Assigned Security Responsibility		Not Applicable
164.308 (a)(3)(i)	Workforce Security		Not Applicable
164.308 (a)(3)(ii)(A)	Authorization and/or Supervision	Workforce Security	Not Applicable
164.308 (a)(3)(ii)(B)	Workforce Clearance Procedure	Workforce Security	Not Applicable
164.308 (a)(3)(ii)(C)	Termination Procedures	Workforce Security	Not Applicable
164.308 (a)(4)(i)	Information Access Management		
164.308 (a)(4)(ii)(A)	Isolating Health Care Clearinghouse Function	Information Access Management	Supports
164.308 (a)(4)(ii)(B)	Access Authorization	Information Access Management	Supports

REQUIREMENT ID	IMPLEMENTATION TOPIC	HIPAA STANDARD	APPLICABILITY TO VMWARE TECHNOLOGIES
164.308 (a)(4)(ii)(C)	Access Establishment and Modification	Information Access Management	Supports
164.308 (a)(5)(i)	Security Awareness and Training		Not Applicable
164.308 (a)(5)(ii)(A)	Security Reminders	Security Awareness and Training	Not Applicable
164.308 (a)(5)(ii)(B)	Protection from Malicious Software	Security Awareness and Training	Supports
164.308 (a)(5)(ii)(C)	Log-in Monitoring	Security Awareness and Training	Supports
164.308 (a)(5)(ii)(D)	Password Management	Security Awareness and Training	Supports
164.308 (a)(6)(i)	Security Incident Procedures		Not Applicable
164.308 (a)(6)(ii)	Response and Reporting	Security Incident Procedures	Not Applicable
164.308 (a)(7)(i)	Contingency Plan		Not Applicable
164.308 (a)(7)(ii)(A)	Data Backup Plan	Contingency Plan	Supports
164.308 (a)(7)(ii)(B)	Disaster Recovery Plan	Contingency Plan	Not Applicable
164.308 (a)(7)(ii)(C)	Emergency Mode Operation Plan	Contingency Plan	Supports
164.308 (a)(7)(ii)(D)	Testing and Revision Procedure	Contingency Plan	Not Applicable
164.308 (a)(7)(ii)(E)	Applications and Data Criticality Analysis	Contingency Plan	Not Applicable
164.308 (a)(8)	Evaluation		Not Applicable
164.308 (b)(1)	Business Associate Contracts and Other Arrangements		Not Applicable
164.308 (b)(3)	Written Contract or Other Arrangement	Business Associate Contracts and Other Arrangements	Not Applicable
164.310	Physical Safeguards		
164.310 (a)(1)	Facility Access Controls		Not Applicable
164.310 (a)(2)(i)	Contingency Operations	Facility Access Controls	Not Applicable
164.310 (a)(2)(ii)	Facility Security Plan	Facility Access Controls	Not Applicable
164.310 (a)(2)(iii)	Access Control and Validation Procedures	Facility Access Controls	Not Applicable
164.310 (a)(2)(iv)	Maintenance Records	Facility Access Controls	Not Applicable
164.310 (b)	Workstation Use		Supports
164.310 (c)	Workstation Security		Supports
164.310 (d)(1)	Device and Media Controls		Not Applicable
164.310 (d)(2)(i)	Disposal	Device and Media Controls	Not Applicable
164.310 (d)(2)(ii)	Media Re-use	Device and Media Controls	Not Applicable
164.310 (d)(2)(iii)	Accountability	Device and Media Controls	Supports
164.310 (d)(2)(iv)	Data Backup and Storage	Device and Media Controls	Supports
164.312	Technical Safeguards		
164.312 (a)(1)	Access Control		Applicable
164.312 (a)(2)(i)	Unique User Identification	Access Control	Applicable
164.312 (a)(2)(ii)	Emergency Access Procedure	Access Control	Applicable
164.312 (a)(2)(iii)	Automatic Logoff	Access Control	Applicable
164.312 (a)(2)(iv)	Encryption and Decryption	Access Control	Applicable
164.312 (b)	Audit Controls		Applicable
164.312 (c)(1)	Integrity		Not Applicable
164.312 (c)(2)	Mechanism to Authenticate Electronic Protected Health Information	Integrity	Not Applicable
164.312 (d)	Person or Entity Authentication		Applicable
164.312 (e)(1)	Transmission Security		Applicable
164.312 (e)(2)(i)	Integrity Controls	Transmission Security	Applicable
164.312 (e)(2)(ii)	Encryption	Transmission Security	Applicable
164.314	Organizational Requirements		
164.314 (a)(1)	Business Associate Contracts or Other Arrangements		Not Applicable
164.314 (b)(1)	Requirements for Group Health Plans		Not Applicable
164.314 (b)(2)(i) - (iv)	Plan Documents	Requirements for Group Health Plans	Not Applicable
164.316	Policies and Procedures and Other Documentation Requirements		
164.316 (a)	Policies and Procedures		Not Applicable
164.316 (b)(1)(i)	Documentation		Not Applicable
164.316 (b)(2)(i)	Time Limit	Documentation	Not Applicable

REQUIREMENT ID	IMPLEMENTATION TOPIC	HIPAA STANDARD	APPLICABILITY TO VMWARE TECHNOLOGIES
164.316 (b)(2)(ii)	Availability	Documentation	Not Applicable
164.316 (b)(2)(iii)	Updates	Documentation	Not Applicable

Table 2: HIPAA Security Rule Standards and VMware Applicability Mapping

Figure 6 diagrams the percent of coverage for HIPAA Security Rule standards that are addressable by VMware and VMware Partner technologies. VMware and partner capabilities are primarily aligned to technical standards. The remaining gaps in capabilities, represented in blue in this diagram, may be filled by the covered entity through other means, but not limited to, business associate contracts and agreements, policies, documented procedures, training, infrastructure diagrams and documentation, management structure, control processes, physical security measures, personnel hiring practices, management procedures and other covered entity control techniques.

HIPAA Security Rule Standards

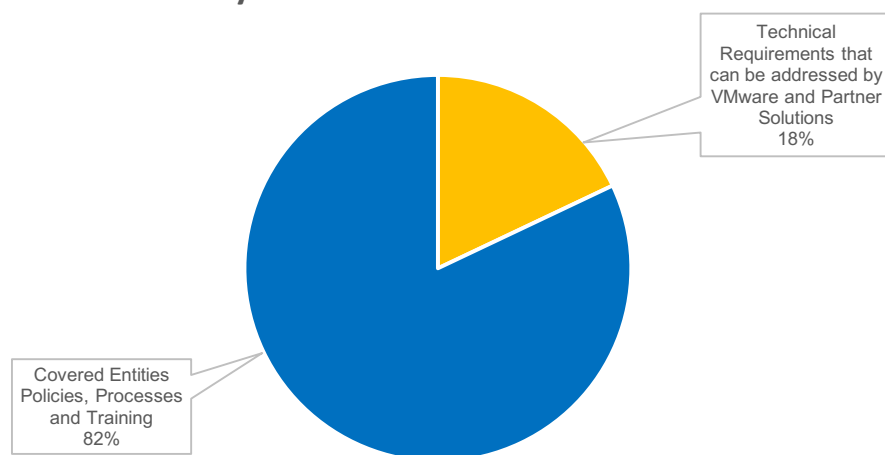


Figure 7: VMware and Partner Solution Coverage of HIPAA Security Rule Standards

Table 3 illustrates a breakout of coverage by VMware Solutions, Partner Solutions and the Covered Entity by HIPAA Security Rule safeguards. Primarily of note is the coverage capabilities in row three relevant to technical safeguards.

PIE CHART	HIPAA SECURITY RULE SAFEGUARDS	% ADDRESSED BY VMWARE SOLUTIONS	% ADDRESSED BY VMWARE PARTNER SOLUTIONS	% ADDRESSED BY COVERED ENTITY
	Administrative Safeguards	5	5	90
	Physical Safeguards	8	10	82
	Technical Safeguards	20	40	40



PIE CHART	HIPAA SECURITY RULE SAFEGUARDS	% ADDRESSED BY VMWARE SOLUTIONS	% ADDRESSED BY VMWARE PARTNER SOLUTIONS	% ADDRESSED BY COVERED ENTITY
	Organizational Requirements	0	0	100
	Policies and Procedures and Documentation Requirements	0	0	100

Table 3: HIPAA Safeguards as Addressable by VMware, Partners and the Covered Entity

VMware Control Capabilities Detail (By HIPAA Security Rule)

This section will only contain the HIPAA Security Rule standards that are relevant to the VMware Solutions in scope for this assessment. It is assumed that standards not covered in this section are addressable by other means. Furthermore, it is not assumed that one technology could possibly meet all of the control requirements for a HIPAA Security Rule Safeguard standard. Where technology is highlighted for capability to address or support a control objective, it is recommended that the covered entity evaluate any additional policies, procedures, standards, training, guidelines and risk are associated in order to more fully address the objective of the control.

Administrative Safeguards 164.308

Security Management Process

164.308 (a) (1) (ii) (A) Risk Analysis

HIPAA Standard Description: 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.

VMware Applicability

It is a requirement for a HIPAA covered entity and business associate to prepare a risk analysis and assessment to identify vulnerabilities and potential risks to the confidentiality, integrity, and availability of electronic protected health information (ePHI). The in-scope VMware systems are not specifically designed to perform risk assessment; however, the integrated approach to the VMware vCloud architecture provides greater assurance of security over many traditional disjointed infrastructures. The combination of software-based platform services to supply storage, compute, and networking and integrated cloud management solutions enables greater awareness for the state of the infrastructure. The holistic solution offered by VMware is capable of enabling tighter controls and multiple layers of control to better protect ePHI.

Risk Management and Assessment are part of HIPAA Security Rule Administrative Safeguards. The defined responsibilities do not necessarily require technology to support the effort. However, technologies such as vRealize Configuration Manager are able to support continuous awareness of risk with respect to adherence to covered entity or business associate compliance to defined policies, procedures and standards. With regards to supporting risk assessment and providing a continuous awareness of risk with existing configurations, VMware vRealize Configuration Manager is capable of discovering the organizations infrastructure, including networks, hypervisors, virtual machines and physical servers. VMware vRealize Configuration Manager is capable of collecting and analyzing information about many systems both physical and virtual including vSphere ESX and ESXi servers, Virtual Machines (VMs), x86 and x64 Windows Servers, x86 and x64 Linux or Unix, Mac, Windows workstations, and Active Directory. Once discovered, these components of the infrastructure can be assessed against well-defined standards or best practices to determine a baseline security posture relative to these

standards. The built-in standards and best practices include vendor-supplied infrastructure hardening guides, common compliance frameworks and configurable organizationally defined and mandated security standards. Additionally, vRealize Configuration Manager is capable of determining patch levels of all managed devices to identify devices that are out of scope for the covered entity or business associates policy. VMware vRealize Configuration Manager is capable of comparing the configuration of the covered entities infrastructure against these baseline standards to quickly identify out-of-compliance configurations. When deployed in the covered entities environment this solution is able to effectively support continuous audit of the virtual, cloud and physical components configurations. Perhaps one of the primary vulnerabilities to remediate are those relative to poor configurations or undetected configuration changes that don't meet compliance objectives. Notification can be sent to specified personnel when systems are found to be out of compliance. Additionally, automatic remediation can be made for the out-of-compliant system to enforce compliance.

VMware vRealize Operations delivers intelligent operations management with visibility from application to storage across physical, virtual and cloud infrastructures. With built in predictive analytics and Smart Alerts, vRealize Operations is able to proactively identify and remediate issues. Performance, capacity, configuration, and compliance are parts of a range of issues that can be identified through analysis with vRealize Operations. Policy-based automation helps to ensure that systems operate within acceptable tolerances and maintain compliance. In addition to ensuring compliance for existing platform components and virtual machines, vRealize automation can ensure that newly deployed infrastructure or virtual machines within in the environment include all the necessary configuration settings and safeguards present to ensure compliance and protect ePHI.

Additional Considerations

Though some of the VMware vRealize Operations Suite solutions are capable of facilitating the identification and analysis of technical risk present with the configuration of the infrastructure, use of the Suite cannot fully identify all risks that challenge the covered entity or business associate. The capability of these solutions is limited to the pre-defined standards, compliance framework technical requirements and existing covered entity policies and risk mitigation practices. The scope of this requirement includes careful review and analysis beyond what is capable by a technical solution alone. For that reason, a thorough evaluation of the organization's business functions, processes, procedures, policies, standards and practices would be necessary to complete the picture of risk. This product applicability guide primarily focuses on technological enablement of controls to address HIPAA requirements. As a result, it does not specifically address administrative functions, employee training and base of employee knowledge or capabilities. Furthermore, it does not address physical risks that challenge the covered entity and business associate; in which case, controls are required to prevent an intruder from gaining physical access to covered entities locations or systems.

Relevant NIST 800-53 Controls: RA-3, SA-14, PM-1, PM-7, PM-8

164.308 (a) (1) (ii) (B) Risk Management

HIPAA Standard Description: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306 Security Standards: General Rules: (a) General Requirements. Covered Entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of his part. (4) Ensure compliance with this subpart by its workforce.

VMware Applicability

Reasonable is commonly used throughout many of the HIPAA Security Rule safeguard standards. The economic viability of virtualized and cloud solutions along with the security capabilities of these same systems increases the degree to which security is reasonable. The remainder of the safeguards that are addressable either fully or partially demonstrate the capability of the VMware software-defined data center and end user computing platforms to aid in the facilitation of confidentiality, integrity and availability of all electronic protected health information.

Given the resourcefulness of malicious actors, the assumption of trust for everything inside the corporate edge firewall is no longer viable to sufficiently ensure confidentiality, integrity or availability of electronic protected health information (ePHI). VMware NSX is capable of providing segmentation and micro-segmentation of covered entity and business associate



workloads. With built in logical security and networking features identified workloads can be more appropriately isolated from each other. In addition to narrowing scope for audit and compliance, it helps to prevent unauthorized access to critical data and workloads from adjacent non-critical data and workloads. Whereas many organizations maintain a relatively flat internal network, focusing security efforts at the covered entity's or business associate's edge, this strategy does little to protect from malicious activity originating from inside the protected boundaries. VMware NSX helps reduce the risk by facilitating least access and least function with respect to the network. Virtual Network Firewalls with specified policies can be distributed to pre-defined security groups of virtual machines or as granular as the individual virtual machine. This can be performed automatically according to various policy definitions such as IP range, logical switch location, security tag, operating system, workload profile, active directory membership, OU placement and more.

As previously discussed, the products and features available with VMware vRealize Operations are capable of ensuring compliance as it pertains to configuration management, performance, availability and the identification of those associated risks. Through automated policy-based deployment, the existing infrastructure as well as new elements are capable of maintaining the same level of security according to the prescribed measures. Much has been examined and addressed by VMware with respect to system hardening and security practices that ensure that VMware virtualization technologies can be included as a compliant platform for hosting HIPAA regulated workloads.

One of the advantages of a software-defined data center over traditional data center infrastructures is the scalability and agility that virtualization can provide. Automation capabilities allow for new resources to be made available to aid in rapid scalability of the infrastructure. To ensure that the newly deployed hosts in the infrastructure adhere to the compliance standards, the automation process includes steps to ensure that security measures are deployed with the new resources. This deployment process is further augmented by the capability of using digitally signed software packages to ensure the integrity of the ESXi software being deployed to new hardware. Integrated with Intel Trusted Platform Module (TPM) and Intel Trusted Execution Technology (TXT), a host can be attested or measured against a known good host configuration during the boot sequence that ensures the host from hardware through the kernel meets the necessary security requirements and is free of tampering or malware.

A Host Profile is a defined point in time configuration, based on a pre-configured known good host. The Host Profile captures the configuration settings of the known good host and can be used for comparison of all hosts in the environment to determine deviations in configuration. Host Profiles ensures that the pre-defined known good configuration, relative to a trusted reference host is maintained throughout the hosts operating cycle. Hosts that have deviated from the standard set by the approved Host Profile can automatically be remediated to match the known-good-host configuration. This supports change management.

From the hardware platform through the application layer, VMware solutions are architected with security in mind. Starting with the core of virtualization, the hypervisor, vSphere ESXi is a type one hypervisor or bare metal hypervisor. What remains of the kernel is only the necessary elements to control the underlying hardware and manage the guest virtual machines. Without all the weight of a traditional operating system, the surface area for attack is minimized significantly.

Multiple layers of security techniques are at work or capable of being deployed within vSphere. Within ESXi, secure isolation of virtual machines at the virtualization layer including secure instruction isolation, memory isolation, device isolation, and managed resource usage and network isolation are one such layer of security. Another configurable layer of security is the use of SSL to secure management of the virtualized environment. SSL is used to secure communications between components of the virtual infrastructure.

To provide greater security to the core element of virtualization, when integrated with vCenter ESXi is capable of being locked down to prevent direct access to the host. All host interactions are required to be performed through the vCenter management interface where least privilege can be enabled and fine grained, role-based access controls can be implemented.

Additional Considerations

Through VMware's vast partner ecosystem, security solutions that are certified for use with VMware technologies can be tightly integrated and implemented as security measures for the HIPAA regulated environment. To further protect against threats or hazards additional security measures can be deployed including antimalware, antivirus, intrusion detection, intrusion prevention, next generation application firewalls, host-based firewalls and IDS/IPS. To further protect against unauthorized use of data or disclosures of information additional partner solutions can be integrated and deployed including file integrity monitoring, data exfiltration monitoring, and security information and event monitoring.



The scope of this document is limited to technical capabilities. Other organizational, administrative or managerial security measures that can be deployed to protect the integrity, availability and security of ePHI should be considered by the covered entity.

Relevant NIST 800-53 Controls: RA-1, PM-6, PM-9

164.308 (a) (1) (ii) (D) Information System Activity Review

HIPAA Standard Description: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

VMware Applicability

All of the VMware technologies represented in this product applicability guide are capable of supporting the requirements of audit and event log generation. The information that is contained in each of the logs is inclusive of that which is necessary to satisfy the requirements. This includes the type of event that occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event and the identity of the individual(s) or subject(s) associated with the event. The time that the event occurred is provided by a timestamp consistent with the system time where the audit or event log was generated. Additional specificity in the log includes source and destination IP addresses, user/process identifiers, event descriptions, success/fail indicators, filenames involved, and access control or flow control rules invoked. In addition to outcome indicators of success or failure, the results are also able to indicate the state of the impacted information system after the event occurred. In most cases the logs are capable of being reviewed using the available management console. For many of the vCenter integrated and managed components, vCenter provides a mechanism to retrieve, view, and search logs as may become necessary.

VMware vRealize Log Insight collects and analyzes all types of machine-generated log data, e.g., application logs, network traces, configuration files, messages, performance data, system state dumps, and more. It enables administrators to connect to everything in their environment, such as OS, apps, storage, and network devices to provide a single location to collect, store, and analyze logs at scale. Log Insight features an intuitive interface to facilitate interactive searches and deep analytical queries for quick, actionable insights. Log Insight adds structure to unstructured log data. It delivers real time monitoring, search and log analytics. It has a dashboard for stored queries, reports, and alerts, enabling correlation of events across the entire IT environment.

While Log Insight is able to more quickly make sense of massive amount of unstructured data in the form of system, audit and event logs, vRealize Operations collects information relative to structured data or metrics directly from applications revealing historical and real time performance indicators. This can be useful for identifying issues within the environment which allow the administrator or engineer to narrow the focus of remediation to the source of the issue and thus achieve timelier remediation and improved service levels. Integration of Log Insight findings with vRealize Operations can further enhance situation awareness providing focused understanding of relevant event logs to structured metrics data. For improved situation awareness, the correlation of the information from vRealize Operations and vRealize Log Insight allows for improved inventory mapping where vSphere inventory items are directly tagged to events collected by log insight. With this tagging alerting can be performed specifically with regard to the impacted object. These alerts from vRealize Log Insight are now capable of being visualized in the vRealize Operations console producing a visual representation of the event correlated with the metric collected by vRealize Operations. Furthermore, the integration allows for the administrator to easily move between vRealize Operations and Log Insight and vice versa with respect to the object and or events that are being investigated.

Additional Considerations

Additional consideration must be taken by the covered entity and business associate to include, as necessary, the formation of an audit review process including individuals identified for responsibility to review, assess and report on audit records. Moreover, to ensure continuous compliance, it will be beneficial for the covered entity and business associate to establish a continuous monitoring strategy to include identification of key metrics to be monitored, establishment of monitoring frequency as well as assessment of monitoring strategy. The responsibilities of which and for whom is clearly defined as these processes are clearly defined. Covered metrics should include those artifacts that are useful to determine effectiveness of organizations policies, procedures, standards, and training and to identify areas of improvement. As much as is reasonable, metrics should also be included that are common in events and audit logs that indicate the possibility of breach of security.

VMware vRealize Log Insight does not sufficiently provide retention capability to satisfy covered entity requirements for log



retention or tamper resistance. The primary role of Log Insight is for troubleshooting recent or immediate issues. It is a tool for system and network administrators and engineers. The requirements for log retention and tamper resistance is better met by a SIEM solution. These requirements are typically necessary to fulfill compliance requirements that enable historical forensic investigations and evidence of continuity of compliance.

The covered entity and/or business associates must establish incident documentation and tracking procedures including information relevant to the incident including associated logs, impact, forensic evidence, handling, evaluation techniques, and trends. Incident information can be obtained from the aforementioned solutions as well as incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Policies and procedures must also exist to require personnel to report suspected security incidents to the organizational incident response capability within a reasonable amount of time to allow for effective response by the entities security response authorities.

Relevant NIST 800-53 Controls: AC-25, AU-3, CA-7, IR-5, IR-6, SI-4,

Information Access Management

164.308 (a) (4) (ii) (B) Access Authorization

HIPAA Standard Description: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.

VMware Applicability

Often the procedures for authorization or supervision of workforce members involve manual workflows that contain paper trails for request, approval, authorization, implementation and supervision. These paper trails can be inclusive of online static forms, email requests and paper forms among other means. For many organizations these procedural workflows can lack definition, and are difficult to maintain and certify as they have developed over time organically. Finding records of request, authorization and implementation and aligning these records into a cohesive evidence of compliance can be cumbersome and time consuming. VMware vRealize Automation is capable of automating many organizationally standard workflow processes. Commonly this is used for automating regular maintenance routines, regular incident response procedures and the like; however, the API is flexible and adaptable to allow for integration into other technical services such as user provisioning and management. The workflows can be orchestrated in such a way to match the workflow procedures defined by the organization to include steps such as request for access, acknowledgement of request, review of request, authorization of request and implementation of authorized access. Through integration with other VMware and partner solutions additional effort can be made to automate the generation of access reports that are necessary to perform personnel reviews.

Access authorization management also applies to authorization and access between devices on the network. Whether user devices, server devices, or workload tiers, restricting access by need prevents unintentional or intentional malicious access by or from those objects which do not meet the need to know requirement. Much as vRealize Automation can be developed to create workflows for user authorization, it can also be used in coordination with VMware NSX to ensure that when a device is deployed it is deployed with the necessary security measures such as logical network segment, security group, logical firewall policies and advanced security measures applied.

Additional Considerations

Though the capability of automating workflows including access authorization, establishment and modification with regard to integration capabilities with Microsoft Active Directory, it is advisable that such an effort not be considered lightly. The design of the workflow should be consistent with the covered entities' and business associates' already established business processes. The architecture of the solution should be flexible to support future updates to the dependent components. The capability of vRealize Automation is not intended to be a replacement for administrative responsibility for this control. Rather, vRealize Automation is capable enhancing the administrative process.

Relevant NIST 800-53 Controls: AC-21, AC-22, AC-23, AC-24, SA-1, SA-2, SA-3, SA-5, SA-10, SA-11, SA-13, SA-15, SA-16, SA-17

164.308 (a) (4) (ii) (C) Access Establishment and Modification

HIPAA Standard Description: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation,



transaction, program, or process.

VMware Applicability

As a continuation of the capabilities of VMware vRealize Automation for access authorization, access establishment and modification are ongoing steps in the process whereby workflows can be automated to establish authorized access, re-authorize access for modifications as roles and responsibilities change. VMware NSX Edge Gateway provides SSL VPN-Plus to allow remote users access to private networks using an SSL client. Remote users can access servers and applications on the private network according to policy and rights assignments applied to and granted to the user respectively.

All of the VMware products which provide user access for administration or other relevant tasks are capable of being configured for appropriate access necessary to align with the role or responsibility of the individual or the group requiring access to accomplish assigned tasks. Out of the box roles are typical of division of responsibilities that may be found within an organization. Beyond this, in many cases, custom roles or rights can be assigned.

Relevant NIST 800-53 Controls: SC-7, SC-43

Security Awareness and Training

164.308 (a) (5) (ii) (B) Protection from Malicious Software

HIPAA Standard Description: Procedures for guarding against, detecting, and reporting malicious software.

VMware Applicability

Preventative measures are a starting point for guarding against malicious software. A starting point for implementing preventive measures is mitigation of risk through the aforementioned assessment. A good way to mitigate risk is to carry out best practices for the implementation of the IT infrastructure. The application of hardening techniques are partly designed to reduce the surface area of attack and/or reduce the potential impact for attack. Another technique for reducing risk is to implement the practices of least function and least privilege.

The present solutions available from VMware enable the capability for granular, role-based assignment both from the network and through the management user interfaces.

Whereas a typical physical network infrastructure may allow for groups of devices to be segmented into separate VLANs, VMware NSX allows for network security and advanced network security techniques to be deployed for protection as granular as individual virtual machines within the same layer 2 network. This capability of NSX enables the same physical edge protection techniques that protect north and southbound network traffic to now protect intra-virtual machine traffic or east and westbound network traffic.

Virtual machines are only allowed to communicate with each other through a virtual switch. This passage of traffic between virtual machines, even those contained on the same host, allows for greater control of the network traffic. The network infrastructure is enhanced by a VMware NSX-provided virtual firewall that sits between the virtual machine's virtual network interface controller or vNIC and the virtual switch or vSwitch. Policy-based determinations for routing of traffic are made by the stateful virtual firewall to protect virtual machine traffic and route that traffic only to its approved destination. This level of granularity is capable of securing traffic between virtual machines, even virtual machines that exist on the same host in the same Layer 2 network. Because the firewall rules are applied to the vNIC of the virtual machine, the rules are allowed to travel with the virtual machine through vMotion processes ensuring that the security provisions stay with the virtual machine. This continuity of security extends beyond the local data center and can be enabled to allow for the same virtual network security concepts to be extended so that the policies and security measures are present with the virtual machine when migrated to other data centers or when recovered in a disaster recovery site.

Additional capabilities built into the VMware vSwitch include support for IEEE 802.1q VLANs. VLANs enable segmentation of a physical network to prevent virtual machines on the same physical network from communicating with each other unless they exist on the same VLAN.

VMware NSX, additionally, provides APIs to allow VMware partners to develop software solutions to enhance security for the virtualized network. These security enhancements, which can be applied individually to virtual machines, include antivirus/antimalware solutions, layer 4 - 7 next generation application firewalls, and intrusion detection/protection sensors. These seamlessly integrated solutions efficiently provide highly capable advanced protection techniques that make use of



the portability and scalability inherent in virtualized and cloud solutions. This enables the same agility afforded the aforementioned virtual firewall to be extended to the advanced network protection measures.

Whereas NSX provides isolation capabilities at the network layer, VMware ESXi is designed to create secure isolation boundaries for virtual machines at the virtualization layer. Included in this secure isolation capability is secure instruction isolation, memory isolation, device isolation, and managed resource usage and network isolation. Each virtual machine is isolated from one another. While not specifically involved in guarding against malicious software attacks, the nature of the hypervisor's architecture reduces the surface area for attack and presents boundaries at critical areas to prevent impact to the hypervisor or the contained virtual machines.

This isolation techniques employed by vSphere for instructions, memory, I/O, resources, devices and network are enhanced through extensions built into the hardware that are designed for x86 virtualization. The hypervisor uses these extensions to further improve security for the hosted virtual machines.

Extensions built into Intel Processors such as the Trusted Computing Group's Trusted Platform Module (TPM) or Intel Trusted Execution Technology (Intel TXT) managed by vSphere provide a trusted boot platform that verifies the physical hardware and hypervisor configuration during the boot sequence to ensure that the platform has not been compromised by malicious software or hardware tampering.

VMware vSphere uses address space layout randomization (ASLR) to randomize where core kernel modules are loaded into memory. The NX/XD CPU features enable the VMkernel to mark writeable areas of memory as non-executable. Both of these memory protection methods help protect the system from buffer overflow attacks in running code. Additional design consideration that were included in VMware vSphere allow for greater protection from denial of service attacks.

When vSphere hosts are managed by vCenter, vCenter provides the capability to enable lockdown mode to limit the access and functionality to the core of the virtualization infrastructure. Lockdown mode disables login and API functions from being executed directly on the ESXi server, forcing changes to be made through the vCenter interface, which also forces use of vSphere Single Sign-On. VMware vSphere CLI commands from an administration server or from a script cannot be run against the ESXi host in lockdown mode. All of the vSphere API privileges that are associated with root access have been disabled. The host access made available for vCenter to manage the host is provided with an obfuscated and protected vpxuser account. This enables and ensures tighter and more managed control of the ESXi hosts managed by vCenter.

For end-user devices and mobile devices that may be in use in a bring your own device environment, AirWatch Enterprise Mobility Management provides tools for managing laptops, tablets and smart phones to ensure that registered devices are properly protected. Among policies to which these devices must adhere are the inclusion of antivirus or antimalware and the inclusion of endpoint or host-based firewalls. If these measures are not present on a registered device, AirWatch Mobile Device Management can deploy the covered entities' and business associates' chosen solution.

VMware vRealize Configuration Manager is capable of checking for the presence of required software such as antivirus, antimalware, host-based intrusion detection/protection solutions and reporting on non-compliant system. Software packages can be created for each required software and deployed automatically to non-compliant devices, ensuring that devices remain compliant and properly protected.

Additional Considerations

Additional design considerations should be made when deploying a virtualized environment to host ePHI. Following VMware hardening guides and best practices is paramount to securing virtualized infrastructure. Out of the box deployment with default settings is typically not sufficient to ensure that the virtualization or cloud infrastructure has met satisfactory requirements for least privilege or least functionality. For example, the default host security profile for vSphere ESXi hosts for incoming and outgoing connections is all source and destination addresses for required TCP and UDP ports. For this reason, the organization should consider the configurable settings for inclusion or modification necessary to properly secure the infrastructure. The architecture and design considerations made available are useful in general for the protection of any critical information system or data. Examples of these considerations include, but are not limited to, physical separation of the hypervisor management network from that of the virtual machine or workload network and physical and VLAN separation of the vMotion network from the virtual machine network to prevent network snooping of virtual machine traffic.

The root account is necessary for the functions of ESXi. As a result, the root account cannot be removed and replaced with a differently named service account; however, the root account can adhere to password rules for complexity. It is strongly suggested that the root password for ESXi hosts and Linux Kernel-based virtual appliances be set using strong password



complexity requirements. Moreover, it is advisable to change the root account password on a regular basis. VMware partner technologies provide solutions to help manage the root account and proxy access when the root account is needed for troubleshooting that ensures that logged changes are attributable to a named user. It is advisable for the ESXi hosts that are managed by vCenter to be placed in lockdown mode. Additional network segmentation with policy-based security should be applied to limit accessibility to the management interface of the ESXi host to only that which is necessary for regular operations. Where ESXi hosts are implemented as standalone hosts, it is advisable to vault the root account and setup local named user accounts for administrative activities.

Relevant NIST 800-53 Controls: SC-38

164.308 (a) (5) (ii) (C) Log-in Monitoring

HIPAA Standard Description: Procedures for monitoring log-in attempts and reporting discrepancies.

VMware Applicability

All VMware solutions listed in scope for this product applicability guide are capable of generating audit records of logon attempts and subsequent user generated activity. Each component user interface that contains login capability logs its own login attempts and makes that log of activity available for review. Included in the logging is records of successful and also failed logon attempts.

Generated logs for VMware technologies are capable of being retrieved by VMware vRealize Log Insight where the logs can be aggregated and analyzed. Reports on logs are capable of being generated to satisfy reporting and review requirements. Additionally alerts can be setup when thresholds that may indicate discrepancies are triggered.

From an end-user perspective VMware Identity Manager contains a user engagement dashboard which allows administrators to monitor user activity. The dashboard displays who is signed in, which applications are being used, and how often applications are being accessed. VMware Identity Manager allows for the creation of reports to track user and group activities and resource usage.

Additional Considerations

Given that this is an administrative control, the narrative above gives examples of how technology can be used to augment and support administrative activities. The covered entity and business associate will still require procedures for creation of log reports, modification of log reports, review of log reports and reporting on discrepancies, including any remediation or incident response procedures.

Also, where the covered entity and/or business associate requires, as part of its policy, long term retention of logs in a tamper resistant container, the use of a third part SIEM solution is advisable.

Relevant NIST 800-53 Controls: SC-42

164.308 (a) (5) (ii) (D) Password Management

HIPAA Standard Description: Procedures for creating, changing, and safeguarding passwords.

VMware Applicability

The critical infrastructure interfaces and components of the infrastructure, such as management consoles and kernel interfaces, are capable of being configured to ensure that password rules are enforced in keeping with compliance requirements and covered entity defined policies. The account password rules that are capable of being enforced for many of the VMware solutions include minimum and maximum password lengths, minimum and maximum password age, password history, password and/or passphrase complexity. Account lockout thresholds can be set to lock out accounts where incorrect username and password combinations exceed the threshold. As it applies to VMware technologies, this control enforcement is applied to accounts that are local to the identified system and are relevant to the access for that system. For vCenter access, this control is made possible through vCenter Single Sign-On configuration. Additional controls are in place to ensure that secret user credentials such as passwords are encrypted and the input of passwords is not made available in clear text either through the input process or viewable on the screen in clear text.

Additional Considerations

Many of the VMware technologies allow for integration with 3rd party directory services solutions for access account



management, such as Microsoft Active Directory. Where Active Directory is available to the covered entity for integration with the VMware technologies, it is advisable to enable this integration and functionality. This allows for centralized management of user accounts. The user accounts can be enabled for membership in Active Directory Security Groups. The Security Groups can then be tied to built-in or custom defined roles set within the VMware technology configuration. The built-in or custom defined roles can be aligned with specific access rights appropriate to meet the covered entities definition of granular access control.

VMware vSphere Single Sign-On (SSO) can be integrated with Active Directory. For standalone vSphere hosts, the host access can be integrated with Active Directory. Where components are not directly accessible through vSphere SSO, many of those components can also be integrated with Active Directory. For end-user access and portal access to published applications, mobile applications, web applications and published virtual desktops, VMware Identity Manager can also be integrated with Active Directory.

Relevant NIST 800-53 Controls: PL-4

Physical Safeguards 164.310

Workstation Use

164.310 (b) Workstation Use

HIPAA Standard Description: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic PHI.

VMware Applicability

This physical safeguard is primarily around appropriate use policies and procedures. It will be the responsibility of the covered entity to disseminate policies and procedures around the proper use and functions of covered entity end user assets including workstations, laptops, tablets, smart phones and so forth. Moreover, it will be the responsibility of the covered entity to properly train the users on the proper use of workstations. That being said, where it is feasible controls can be enabled for various classes of workstations to enforce policies and procedures and require users to behave in a way that is expected.

VMware Workspace One allows for centralized management of desktops, both physical and virtual. To begin with, pre-built and hardened workstation images can be deployed as virtual machines and run from the confines of the secure data center. Likewise these pre-built and pre-hardened images can be deployed to physical workstations or laptops where the image can run as a localized virtual machine instance or be deployed directly to the hardware. The latter configuration allows for work to be performed offline.

Images can be categorized based on job functions with pre-installed software consistent with the use requirements of the recipient. Using virtual desktops with VMware Horizon enables critical workloads that require a higher level of security to be more tightly controlled in more secure physical environments. These virtual desktops can then be accessed using secure access protocols both from on-site locations as well as from remote locations.

As the virtual desktop is physically secure within the covered entity's or business associate's secure datacenter, tighter network access controls can be enabled using VMware NSX. VMware NSX for vSphere Horizon allows granular network control to be deployed to virtual desktops, similar to the use case with virtualized servers. Policies can be established individually to a virtual desktop or corporately to classes of virtual desktops with definitions to include source and destination addressees and network protocols for incoming and outgoing network traffic. Even in a relatively flat virtual desktop network, virtual desktops would not be able to communicate directly over the network with each other except where permitted by policy. This helps to prevent lateral vectors of attack that are commonly used to search out higher privileged access. Additionally, the same functionality that allows for advanced network security measures to be applied to virtualized servers is also capable of being deployed to virtualized desktops, including antivirus and antimalware solutions, intrusion detection and protection and next generation application firewalls.

Policies can be enabled and executed at the user level or the virtual desktop level to permit or deny the capability to extract or copy data to removable storage devices, internal local storage devices where VDI is used, or cloud based storage.

VMware User Environment Manager offers personalization and dynamic policy configuration across any virtual, physical and



cloud-based environment. User Environment Manager simplifies end-user profile management by providing organizations with a simple and scalable solution that leverages existing infrastructure. IT can map infrastructure (including networks and printer mappings) and dynamically set policies for end users to securely support more use cases. This allows the covered entity and/or business associate to orchestrate boundaries of use around users that align with the user's functions and promote better security.

In addition to mobile device management control, AirWatch Enterprise Mobility Management provides secure remote access capabilities to virtual published desktops, virtual published applications, mobile applications, and data repositories for laptops and mobile devices. A workspace portal is presented to end users from which subscribed applications, services and data are accessible. The subscribed services can be pre-defined based on roles and responsibilities in alignment with the organizationally defined job functions or customized and tailored to an individual's assigned responsibilities.

AirWatch compliance engine continuously monitors devices and performs escalating actions to prevent non-compliance. If a non-compliant device is detected, preconfigured escalating actions are performed automatically to bring the device back into compliance.

AirWatch Enterprise Mobility Management also provides a secure web browser that can be used to provide better security control around access to web application interfaces.

Additional Considerations

Where the possibility that a physical device may be removed and that physical device contains sensitive or protected health information, the physical device should be protected with at rest encryption. Where virtual desktops are capable of being used, the use of thin or zero clients can reduce the surface area of attack by simplifying the hardware and operating system of the end user device down to only what is necessary to securely access the virtual desktop.

Relevant NIST 800-53 Controls: AC-8, AC-9, AC-16, AC-17, AC-19

Workstation Security

164.310 (c) Workstation Security

HIPAA Standard Description: Implement physical safeguards for all workstations that access electronic PHI, to restrict access to authorized users.

VMware Applicability

AirWatch Enterprise Mobility Management Mobile Device Management is capable of enforcing configuration controls on enrolled and registered mobile devices. Control enforcement capabilities of AirWatch mobile device management include: required password or pin for unlocking and securing the device; checking and enforcement of security measures including antivirus and firewalls; code enforcement to include all necessary patches for operating systems and approved applications; application limits; blocking of rooted devices; and disabling or limiting participation with unsecure network protocols or access methods including Bluetooth and unsecure Wi-Fi networks.

Terms of use can be enabled and required for all enrolling devices to require acceptance by the end user prior to participation. The terms of use are able to be customized to match policies established by the covered entity. Whenever version of the terms of use agreements are updated, users are then required to accept the new terms of use reflecting the most recent revisions in the agreement.

From a central console, AirWatch allows for mobility management of Android, Apple iOS, Blackberry, Chromebook, Mac OS, Windows, and peripheral devices from a single management console. This console provides advanced logging and reporting capabilities to support decision making by assigned personnel responsible for maintaining compliance with regard to endpoint devices.

AirWatch Enterprise Mobility Manager grants the capability to track the location of enrolled devices, remotely lock devices, and remotely wipe enrolled devices in order to protect any data or access capability that may be available to the mobile device.

Additional Considerations

Where physical devices are used, it is recommended that the organization also consider methods to prevent tampering with such physical devices. Consideration can be made to further lock down devices to prevent the infiltration. Network security methods should also be used to identify devices on the network as authorized; without the proper authorization, the device is



incapable of obtaining an IP address and subsequently incapable of further network access. Some of the important things to consider are physical locking mechanisms to secure the asset to the location to prevent the asset from growing legs and walking out the door. To ensure the validity of authorized users, the use of multi-factor authentication methods whereby more than one or two variables are used to properly identify users can assist with ensuring that the devices and the subsequent content or applications are only being accessed by identifiable authenticated users. To prevent unauthorized shoulder surfing, additional measures should be put in place to protect the content on the screen such as the use of screen filters or locating screens away from patients.

Relevant NIST 800-53 Controls: AC-7, AC-10, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11, PS-1, SA-18, SA-19, SC-32, SC-41

Device and Media Controls

164.310 (d) (2) (iv) Data Backup and Storage

HIPAA Standard Description: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

VMware Applicability

VMware vSphere Data Protection is a backup and recovery solution integrated directly into vCenter and accessible through the vSphere Web Client. It provides disk based backup of virtual machines and applications. This built-in solution is able to meet the requirement of creating retrievable, exact copies of electronic protected health information when that ePHI is stored within virtual machines in the virtual infrastructure. The backups are capable of being stored locally on the vSphere Data Protection appliance or replicated to other vSphere Data Protection appliances as well as physical backup repositories onsite or offsite as policies may dictate. The backups can be scheduled or run ad-hoc to meet the requirement of performing the backup prior to movement of equipment.

Additional Considerations

Where policies and requirements for exact copy storage replica may be required for forensic evaluation, vSphere Data Protection is not capable of satisfying these requirements.

Relevant NIST 800-53 Controls: MP-4

Technical Safeguards 164.312

Access Control

164.312 (a) (2) (i) Unique User Identification

HIPAA Standard Description: Assign a unique name and/or number for identifying and tracking user identity.

VMware Applicability

All VMware products are capable of assigning unique names and or numbers for identifying and tracking user's unique identities.

For end users, VMware Identity Manager is a service that extends the on-premises directory infrastructure to provide a seamless single sign-on (SSO) experience to web, mobile, SaaS, and legacy applications. Identity Manager can be consumed as a cloud based service or downloaded and installed on-premises. It is integrated with AirWatch Enterprise Mobility Manager to enable seamless SSO to native mobile applications and comes complete with an enterprise app store, SAML identity provider (IDP), application usage analytics, conditional access policy, and more. This capability further enhances the assignment of unique identification for users by simplifying the account management process across multiple platform types. This solution reduces the complexity of account management for end users. By reducing the complexity for end users, adoption and proper application of policy is more likely. Central management of identity increases the supportability of the requirements by administrators.

AirWatch Enterprise Mobility Management includes mobile security features that help to uniquely identify and track the identity of devices that are allowed to participate on the covered entities network. AirWatch enables administrators to prevent unknown devices from connecting to covered entity networks, and configure certificate-based access to corporate VPN and Wi-Fi networks. Network Access Control (NAC) integration, AirWatch VPN On-Demand and AirWatch AppTunnel enable administrators to grant access based on compliance, provide access to internal sites and secure mobile



communications with enterprise networks.

Additional Considerations

Managing local accounts on individual components can be cumbersome and difficult to track as each component local account is independent of the others. Challenges arise when creating new users or disabling departing users, the least of which is the time it can take to enable access. The greater issue is overlooking disabling a granted access at the local level for a terminated user. To improve the management of named user accounts and group membership, it is advisable to integrate or link access rights to a centralized directory service such as Microsoft Active Directory. Named users can be created in active directory and granted membership of Active Directory Groups. The Active Directory Groups can then be linked to or made members of system groups. The system groups as before are linked to specific permissions. This allows for a centralized location to create and enable users.

Relevant NIST 800-53 Controls: AC-1, AC-2, AC-4, AC-5, AC-6, AC-14, CA-9, AI-1, SC-1

164.312 (a) (2) (ii) Emergency Access Procedure

HIPAA Standard Description: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

VMware Applicability

VMware's "One Cloud, Any Application, Any Device" architecture is useful for enabling business to happen anywhere. One advantage of this flexibility is support for disaster recovery. With a software-defined data center and software-defined end-user computing environment, the systems that support the business applications, data and processes are no longer constrained to specific physical locations. They are transportable in as much as network resources exist to support replication and migration and tools are in place to securely manage the process of replication and recovery.

VMware Site Recovery Manager enables a number of disaster recovery options. VMware Site Recovery Manager is the industry-leading solution to enable application availability and mobility across sites in private cloud environments. Site Recovery Manager is an automation software that integrates with an underlying replication technology to provide policy-based management, non-disruptive testing, and automated orchestration of recovery plans. This provides simple and reliable recovery and mobility of virtual machines between sites with minimal or no downtime. VMware Site Recovery Manager is capable of simplifying recovery, and execution of disaster recovery plans with as little as zero downtime while at the same time reducing the cost of ownership for disaster recovery by up to 50%.

VMware vSphere Replication is a hypervisor-based replication technology that can be used with VMware Site Recovery Manager. VMware vSphere Replication provides customizable recovery point objectives and multiple point-in-time recovery options. It is natively integrated with Site Recovery Manager and is included with most vSphere editions. An alternative to vSphere Replication, many storage providers also supply storage based replication technologies. VMware Site Recovery Manager uses storage replication adapters developed by third party storage partners to integrate with the array based replication and stretched storage solutions. This flexibility for replication combined with Site Recovery Manager enables application for many disaster recovery use cases.

VMware has available disaster recovery services that can be extended to its VMware customers searching for a site to facilitate business continuity. The services provided through vCloud Air enable the covered entities of a VMware solution centric software-defined data center to extend to its own facilities. This allows the covered entity to extend storage, network and compute virtualization to the disaster recovery site and maintain the same controls, policies and functions built into its private site.

VMware vSphere Data Protection is capable of being used to support or augment procedures for obtaining necessary electronic health information during an emergency. Whereas vSphere Data Replication and vCenter Site Recovery Manager are able to achieve near zero recovery point objective (RPO) and recovery time objective (RTO), not all workloads may be required to meet this level of recovery objectives. Data Protection is a built-in backup solution capable of meeting desired schedule requirements for backup and retention. Data Protection Appliances are able to replicate protected data to offsite repositories, such as a disaster recovery site where data can be restored to virtual infrastructure at that location. From this backup repository virtual machines can quickly be restored, even when vCenter is unavailable.

A workforce strategy that involves virtualized desktops and mobility not only improve the security and control of the



endpoints, it also presents an excellent strategy for disaster recovery and business continuity. Virtualized desktops, applications, and mobile applications are virtually capable of being hosted in any data center. Just as the software-defined data center enables agility, extensibility and portability for server systems, VMware Horizon Enterprise Edition grants entities the flexibility to distribute or extend the virtual desktops across multiple data centers. Combined with VMware Horizon Air, the capability to incorporate cloud services into the entities desktop management structure supplies flexibility necessary to respond quickly in a disaster scenario. When incorporating VMware Horizon Workspace Suite into daily production operations and extending the production implementation to a disaster recovery site, the method for access becomes seamless whether in operations as normal or in disaster recovery.

Additional Considerations

Regardless of the extent of procedure automation with regard to disaster recovery, policies, procedures, training, and testing, are necessary components of any successful business continuity and disaster recovery plan. Managerial definition for disaster declaration and organizational procedures for executing disaster recovery protocols are more examples of important steps of planning and execution. The organization may have various definitions for declaration of disaster with varying response procedures with criteria for declaration based on numerous key variables.

To support emergency response and actions to be undertaken to ensure that ePHI is continuously available there may be a number of actions that will take place prior to bringing up a disaster recovery site in full. To manage emergency response, the covered entity may implement response controls such as redundant power, generator backup power, battery backed power to facilitate a clean transfer of power. Multiple redundant internet service providers may be used to facilitate continuity of service in the case of a single service failure. The extent that adequate protective measures are implemented to increase the availability of the primary production site, the likelihood of common disasters can be reduced significantly.

Beyond those things outside the immediate capabilities of VMware technologies, VMware offers increased availability for critical virtual machines and data including VMware vSphere High Availability. VMware vSphere High Availability delivers the availability required by most applications running in virtual machines. This is a uniform, cost effective failover protection mechanisms against hardware and operating system outages. VMware vSphere Fault Tolerance provides an improved failover capability for failed virtual machines. Fault Tolerance enables continuous availability of applications in the event of server failures by creating a live shadow instance of a virtual machine that is always up-to-date with the primary virtual machine. Unlike High Availability which reboots virtual machines in the event of a host failure, in the event of a failure of the active primary node, Fault Tolerance triggers an automatic failover to the secondary virtual machine without any downtime.

Relevant NIST 800-53 Controls: CP-1

164.312 (a) (2) (iii) Automatic Logoff

HIPAA Standard Description: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

VMware Applicability

All vSphere consoles and interfaces are configurable to allow for idle session timeout, whereby, the idle session is disconnected and/or logged off. The amount of allowed idle time is configurable in most cases to address the policy requirements of the covered entity. Once the session idle timeout has expired, the user is required to reconnect or re-login to the session by providing the necessary credentials as if the user was logging in for the first time.

Relevant NIST 800-53 Controls: AC-11, AC-12, SC-10

164.312 (a) (2) (iv) Encryption and Decryption

HIPAA Standard Description: Implement a method to encrypt and decrypt electronic protected health information.

VMware Applicability

Through VMware's network of partners, integrated solutions are available to enable encryption and decryption of electronic protected health information that is created, stored, processed and transmitted in a VMware environment. Data at rest solutions exist to provide encryption capability for virtual machines and the contained virtual machine disks and data. These encryption solutions protect the data and deny the ability for unauthorized exfiltration of the virtual machine from the trusted environment. Other solutions enable encryption for transmitted data ensuring that the data is not capable of being



intercepted in a readable fashion while it is in transit. All of these encryption solutions make use of Intel AES-NI to improve the performance of encryption that otherwise would make its implementation infeasible from a performance standpoint.

Additional Considerations:

Relevant NIST 800-53 Controls: SC-12, SC-13

Audit Controls

164.312 (b) Audit Controls

HIPAA Standard Description: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

VMware Applicability

All of the VMware technologies are capable of keeping a record of the information systems activities. The records that are created are consistent with best practice requirements for determining the date and time of the activity, the person or service that was associated with the activity, the description of the activity, and the outcome or results from the activity. The logs are capable of being retrieved by or sent to a syslog service or a SIEM solution.

VMware vRealize Log Insight, a part of vRealize Operations - Enterprise, is able to obtain records of activities from VMware systems and examine the records for activities as specified by the covered entity. It is also capable of examining the records to discover issues that may indicate inability to meet service level agreements, probability for failure, performance issues, service failures and more. This improves the response time for information system incidents by automating the examination and review process. Alerts and notifications can be delivered to designated personnel on specific triggers of activity. This allows the covered entity to respond quickly to the things that matter.

Additional Considerations

VMware vRealize Log Insight's primary purpose is to aid in discovery and troubleshooting of technical issues as it relates to the VMware Infrastructure. The outcomes from the use of vRealize Log Insight are most likely relative to improved service levels, faster mean time to resolution, consistency in operation and performance of the virtualization infrastructure. The solution is capable of retaining logs for a longer period of time than the individual VMware virtualization components from which it collects the logs. It is not intended to meet regulatory requirement specific to retention requirements, nor maintaining the logs in an unalterable, tamper resistant repository. Partner solutions exist that are capable of being integrated with the VMware virtualized environment that meet or exceed these regulatory requirements.

Relevant NIST 800-53 Controls: AU-1, AU-2, AU-4, AU-5, AU-6, AU-7, AU-8, AU-9, AU-11, AU-12, AU-13, AU-14, AU-15, AU-16, CA-5

Person or Entity Authentication

164.312 (d) Person or Entity Authentication

HIPAA Standard Description: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

VMware Applicability

VMware solutions are capable of integration with multi-factor authentication mechanisms. Support exists where authentication is configured through Microsoft Active Directory to enable additional factors of authentication beyond user name and password. For access to infrastructure service and management consoles as well as self-service portals, this integration allows for additional authentication parameters such as authentication keys and tokens.

In addition to providing application provisioning, end-user self-service catalog, and conditional access controls, VMware Identity Manager also provide Single Sign-On for software-as-a-service SaaS, web, cloud and native mobile applications. This Single Sign-On solution for end users enables SSO with an included identity provider or is capable of being integrated with existing identity providers.

VMware Identity Management with Adaptive Access can establish authentication trust with mobile devices through included AirWatch device registration and console. This allows for establishing trust between users, devices and the cloud for conditional access controls.



Additional Considerations

The covered entity should determine, as is feasible, what methods of authentication should be used to protect the infrastructure as well as the data contained therein. Those methods of authentication should be implemented in such a way that users are properly trained in the use of and the protection of authenticators. Additionally, when properly deployed, the private encryption keys which support authentication methods should be properly secured to ensure that the keys are not capable of being tampered with or removed from the secure trusted container.

Relevant NIST 800-53 Controls: IA-2, IA-3, IA-4, IA-8, IA-9, IA-10, IA-11

Transmission Security

164.312 (e) (1) Transmission Security

HIPAA Standard Description: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

VMware Applicability

VMware vSphere Distributed Switches (vDS) are capable of being configured to assign ports on the virtual switch to a port group. The port group can be assigned to a specific network VLAN and/or private VLAN. Through this capability virtual machine communications within a host or cluster of hosts can be limited.

VMware NSX is capable of enabling transmission security by enabling segmentation and micro-segmentation of networks. Policies are enabled to enforce restrictions to and from networks and network devices to prevent unauthorized access over the virtualized lines of transmission. These network access controls can be enforceable to network segments, applications, virtual machines and/or users. As previously discussed, VMware NSX is also capable of being integrated with additional network security measures provided by VMware partners such as intrusion prevention, intrusion detection, next generation firewalls, and antivirus and antimalware solutions.

VMware NSX also supports multiple VPN based access methods to the virtual environment. VPN can be enabled to support site to site connections as well as SSL VPN connections for end users into the environment. This IPSEC solution can provide both authentication and encryption mechanisms to grant access to the cloud environment and then only to those segments of the environment that are authorized.

VMware Horizon and AirWatch Enterprise Mobility Manager enable containerized secure access to apps and data. Access to sensitive apps and data is only available within the confines of the secure container. In this case, users only need to be concerned with curious shoulder surfers and would be required to have controls in place to minimize this activity.

Additional Considerations:

Relevant NIST 800-53 Controls: NA

164.312 (e) (2) (i) Integrity Controls

HIPAA Standard Description: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

VMware Applicability

Primarily in scope for this HIPAA Security Rule Safeguard standard is file integrity monitoring (FIM). VMware technologies are not in scope to provide this level of control to measure the integrity of ePHI. While there are capabilities with VMware and partner technologies to validate the integrity of configuration settings and files for supported systems, this control is primarily concerned with the protection of health information. By extension, it can be supposed to some extent that the underlying infrastructure systems should maintain integrity to prevent subversion of controls in place for the protection of the data that is stored within the virtual infrastructure.

Inasmuch as the integrity of the underlying systems is important to the integrity of the data contained therein, it would be necessary to ensure that proper mechanisms are in place to equally ensure the integrity of those systems. For the systems itself, VMware vRealize Configuration Manager is capable of inspecting the components of the virtual infrastructure up through and including the virtual machine operating system. To properly ensure integrity, vRealize Configuration Manager not only checks against baseline known good configurations of those systems, but is also capable of ensuring proper



deployment of security patches and updates.

VMware NSX contains a firewall capable of stateful packet inspection. Rules by default are capable of being enforced to deny all traffic except where specific exceptions are documented and implemented.

Additional Considerations

Relevant NIST 800-53 Controls: AC-18, AU-10, SC-2, SC-3, SC-4, SC-8, SC-11, SC-16, SC-18, SC-19, SC-20, SC-21, SC-22, SC-28, SC-29, SC-40, SI-1, SI-7, SI-10, SI-11, SI-12, SI-14

164.312 (e) (2) (ii) Encryption

HIPAA Standard Description: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

VMware Applicability:

Additional Considerations:

Relevant NIST 800-53 Controls: NA

Summary

There is no doubt that the transformation of business to the digital world presents exciting opportunities for businesses around the world. New businesses have emerged in recent years that have shifted the paradigm for how things are traditionally done. Among these transformations is the concept introduced by VMware of “One Cloud, Any Application, Any Device” architecture. Alone, this capability presents opportunities for improvements in how people interact with information. Improvements in speed and the availability of information can assist people in business and the health care industry with making informed decisions. This flexibility also presents the possibility for greater risk. It isn’t uncommon for security to follow in the footsteps of a brave new frontier as the awareness for the need of security paces behind the benefit for the new technology. Even with the benefits from accelerated innovation and mobile cloud applications, security of electronic protected health information is still of utmost concern. This product applicability guide identified ways in which VMware’s software-defined data center and end-user computing platforms help to govern risk and support a responsible participation in ongoing and continuing innovation.

Appendix A (HIPAA Security Rule)

<http://www.hhs.gov/hipaa/for-professionals/security/index.html>

Appendix B (What is Cloud)

<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

<http://www.vmware.com/files/pdf/VMware-Public-Cloud-Service-Definition.pdf>

<http://www.vmware.com/files/pdf/vcat/Private-VMware-vCloud-Service-Definition.pdf>

Appendix C (Product Listing)

For more information about the products listed in this guide, please visit www.vmware.com. Due to the frequency that links and documents change with regard to these products, precise URLs are not provided.

Glossary of Terms

HIPAA – Health Insurance Portability and Accountability Act

HIPAA Security Rule – establishes national standards to protect individual electronic personal health information that is created, received, used, or maintained by a covered entity and/or business associate. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic protected health information.

HITECH – Health Information Technology for Economic and Clinical Health Act

Omnibus Rule – The U.S. Department of Health and Human Services (HHS) Office for Civil Rights announces a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

ePHI – electronic protected health information

SDDC – Software Defined Data Center is a data storage facility in which all elements of the infrastructure including network, storage, compute and security are virtualized through software and delivered as a service.

EUC – End User Computing

Bibliography

Much of the content that informed this paper came from commonly accessible materials found at www.vmware.com and www.hhs.org.

Acknowledgements

VMware would like to recognize the efforts of the VMware Center for Policy & Compliance, VMware Partner Alliance, and the numerous VMware teams that contributed to this paper and to the establishment of the VMware Compliance Program. VMware would also like to recognize the Coalfire Systems Inc. VMware Team

www.coalfire.com/Partners/VMware for their industry guidance. Coalfire®, a leading North American Electric Reliability Corporation Critical Infrastructure Protection, Version 5 (NERC CIP v5) firm, provided the guidance and control interpretation described herein.

The information provided by Coalfire Systems and contained in this document is for educational and informational purposes only. Coalfire Systems makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein.

About Coalfire

Coalfire (Coalfire Systems, Inc.) is the trusted leader in cybersecurity risk management and compliance services. Coalfire integrates advisory and technical assessments and recommendations to the corporate directors, executives, boards, and IT organizations for global brands and organizations in the technology, cloud, healthcare, retail, payments, and financial industries. Coalfire's approach addresses each businesses' specific vulnerability challenges, developing a long-term strategy to prevent security breaches and data theft. With offices throughout the United State and Europe, Coalfire was recently named one of the top 20 Most Promising Risk Management Solution Providers. www.coalfire.com



Disclaimer

* VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided "AS IS". VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of an actual Cyber Security auditor or competent legal counsel.