VMware vCloud® for Healthcare and HIPAA/HITECH

WHITE PAPER

vmware®

Table of Contents

Executive Summary

Heavily regulated industries such as healthcare face unique information technology challenges. While driving down costs and improving the quality and delivery of patient care, healthcare providers must comply with a growing number of government mandates and rapidly changing industry practices surrounding the privacy and security of personal health information (PHI). With looming deadlines, such as meeting the Health Information Technology for Economic and Clinical Health (HITECH) Act meaningful use requirements, healthcare providers are looking to virtualization and cloud computing to provide the flexibility and efficiency benefits they need to meet their agility and compliance goals, at lower cost.

But not all cloud solutions are designed to deliver what is truly needed—and only one solution provides a complete and integrated cloud infrastructure that can help meet stringent Health Insurance Portability and Accountability Act (HIPAA) and HITECH requirements. VMware vCloud® for Healthcare transforms the cost, quality and delivery of patient care **and** provides the necessary control and transparency for regulated healthcare organizations to establish and maintain HIPAA and HITECH compliance in their virtual and cloud environments.

Examining Virtualization, Cloud and Healthcare IT

Virtualization has been a longtime trend in information technology. Early adopters concentrated resources on large dedicated hardware platforms such as mainframes. Then VMware pioneered the common practice of subdividing centralized resources using virtual-machine software to help organizations across industries lower capital expenses and maximize the use of their computing resources. Virtualization has since been extended to servers, network devices, storage and desktops—and it is widely regarded as the foundation for cloud computing.

With support for virtualization from the world's leading electronic medical record (EMR) and medical imaging vendors, healthcare IT has accelerated its adoption of virtualization—and cloud computing—to help power even the most critical patient-care systems. Yet today, some providers remain skeptical that virtual and cloud infrastructure can adequately address their unique security and compliance requirements.

The primary reasons for their skepticism are

- **Ever-changing government-mandated security and compliance requirements** – Forced to deploy critical systems on isolated, dedicated physical devices—with every application vendor typically requiring its own unique hardware and software stack—IT teams are challenged to support continually unforeseen changes in healthcare IT environments where processes are complex, time-consuming and manual.
- **Complex relationships between disparate clinical applications** – Healthcare IT teams have the difficult task of managing information flows between large numbers of integrated and interfaced applications that all share PHI to create a consolidated patient record.
- **Increasingly mobile caregivers** – Laptops, tablets and other mobile devices are becoming preferred methods of information access for busy, on-the-go physicians, and physicians' increasing mobility is making it difficult for IT teams to provide secure and compliant access from a growing variety of endpoint devices.

To overcome these obstacles, healthcare providers are adopting virtualization and vCloud for Healthcare to help their IT teams better manage complete system support while ensuring continuous compliance. Virtualization creates pools of virtual hardware resources and provides secure, compliant logical partitions. With logically partitioned critical-care systems on fewer, more powerful and intelligent servers and devices, IT administrators can remove complexity and enhance security, because they are introducing a centralized management layer between the hardware and care systems. Using virtualization as a means to deliver patient-care systems enables a consolidated view of risk, a key capability for effective compliance.

In hospitals around the world, virtualization benefits are also extending to the point of care. Virtual desktop infrastructure (VDI) solutions, such as VMware® AlwaysOn Point of Care™, provide secure and mobile access to patient-care systems, enabling clinicians and caregivers to securely access patient data from nearly any device inside or outside their hospital. Remote clinics and employees, including ICD-9 and ICD-10 coders, also benefit by gaining reliable, consistent access to all applications available to them in a virtualized workspace.

The primary concern for healthcare IT will always be providing continuous patient-care services. As specific services are delivered, however, IT teams must now ensure that they can account for every patient data detail as it is accessed and updated by various caregivers—or face brand-damaging, public penalties and fines. To meet these stringent PHI requirements, healthcare IT teams need a complete, integrated, industry-focused virtual and cloud infrastructure solution that supports always-available applications, changing requirements and compliance mandates across mobile workstations and the data center.

Reviewing HIPAA and HITECH

As most healthcare providers know, when HIPAA was enacted in 1996, it called for administrative, technical and physical controls for PHI (defined as any identification or information related to a person's health, treatment or payment for services). Later, because of computerized physician order entry (CPOE) systems, HIPAA was expanded to include electronic personal health information (ePHI)—the transmission of PHI created, received and maintained electronically.

When the HIPAA rules were updated in 2009 by a section of the American Recovery and Reinvestment Act (ARRA) titled the HITECH Act, major changes included increasing financial penalties, broader definition of scope for compliance (e.g., Business Associate Agreement) and a breach disclosure requirement for any incident involving more than 500 patients. Since the rules were finalized and a specific body has been providing oversight, many expensive, high-profile fines have been assessed.[1]

With PHI at the heart of both HIPAA and HITECH, healthcare providers need to establish a clear scope as a foundation for audits, notifications and disclosures. Because PHI involves not only technology, but also the people and tasks involved in storing, processing or transmitting data, HITECH states that all health service entities that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use or disclose PHI in either paper or electronic form (e.g., EMRs) must be regulated. At a high level, the following entities are included: healthcare providers, healthcare clearinghouses, health plans and business associates—all of which can benefit from vCloud for Healthcare to help establish HIPAA- and HITECH-compliant infrastructures.

Introducing vCloud for Healthcare

The value of virtualization to reduce capital and operating expenses is readily apparent, with more than half of x86 physical servers already virtualized. Yet vCloud for Healthcare goes beyond traditional cost savings to support the entire healthcare IT environment—from point-of-care applications to the most critical patient-care systems.

Hospitals of all sizes can benefit from vCloud for Healthcare, the only fully featured and integrated solution to include everything healthcare IT needs for building and managing agile, reliable cloud infrastructure that helps transform the cost, quality and delivery of patient care (see Figure 1). vCloud for Healthcare includes technologies that address critical healthcare IT concerns:

- **Clinical point of care** – Save time and improve workflows with secure authentication (e.g., the touch of a finger or tap of a badge) to clinical workspaces and patient-care applications (required for meaningful use).
- **Application management and catalog services** – Streamline processes with efficient self-service access and management of approved end-user applications.
- **Mobility collaboration** – Improve connected care with access to patient-care applications, including EMRs and CPOE systems, from any device, anywhere.
- **Care systems analytics** – Reduce downtime of critical patient-care applications and remediate issues before they affect end users (required for meaningful use).
- **Industry security compliance** – Enable proactive regulatory compliance for the cloud and deliver dynamic clinical IT services in a trusted infrastructure.

1 More information about HIPAA breaches, rules, fines and affected providers can be found on the U.S. Department of Health and Human Services Web site.

- **Care systems continuity** – Keep systems up and running (required for meaningful use).
- **Care systems automation** – Improve efficiency by simplifying and automating IT operations.
- **vCloud Connector for healthcare**– Help ensure that regulated workloads can be safely moved to public clouds by means of a hybrid model.
- **Care systems application manager** – Deploy, monitor and scale multitier healthcare applications.

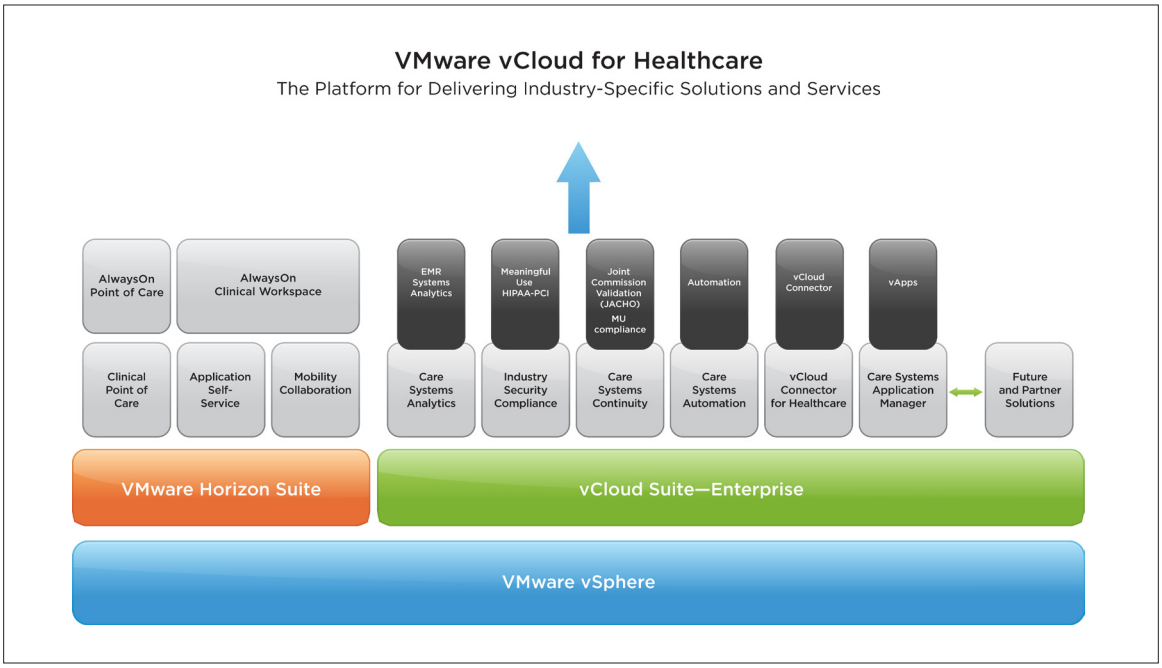

Figure 1. Transforming the Cost, Quality and Delivery of Patient Care While Enabling Proactive Compliance for the Cloud

Overcoming Security and Compliance Obstacles

With vCloud for Healthcare, IT teams can continue to provide the highest quality care while easily and continually assessing, remediating and verifying changes to systems to meet governance, risk, security and compliance requirements. In contrast to antiquated scanning methodologies or separate tools and processes that run at intervals and create gaps in the compliance process, vCloud for Healthcare uses automation to continually inspect, discover and lock down healthcare IT environments. It offers a simple, one-click method for quickly remediating issues and bringing a system back into compliance, and it offers verification to complete the compliance life cycle—a process that begins again as soon as the previous cycle concludes.

By delivering codified knowledge through policy-driven configuration management—whereby approved operating-system images and software packages and patches are added and removed—vCloud for Healthcare can reduce provisioning time and operational costs while helping to support compliance. It enables healthcare IT to quickly, continuously and automatically baseline, review and remediate clinical systems in the environment, proactively gaining thorough security and compliance coverage at lower cost. vCloud for Healthcare also enables organizations to more quickly and thoroughly audit appropriate requirements for meaningful use related to PHI.

vCloud for Healthcare can help healthcare IT quickly and efficiently modernize legacy applications and infrastructure while achieving meaningful use targets fulfilling HIPAA compliance and ultimately improving patient outcomes. Together with AlwaysOn Point of Care, which secures the clinical desktop and enables caregivers to practice medicine, not IT security, vCloud for Healthcare manages the service levels required to obtain better patient outcomes and

- Establish a trusted zone for PHI
- Scan for sensitive data

- Enable continuous configuration compliance
- Remove the endpoints, preventing data theft or loss

VMware vSphere®, the foundation of vCloud for Healthcare, is built to support the broadest range of virtual and cloud infrastructure needs, and has been broadly adopted by hospitals of all sizes—ranging from the largest multifacility systems to critical-access facilities. KLAS-rated vSphere has more than 80 percent market share in healthcare virtualization.[2] Moreover, VMware and the VMware Partner Network—including more than 55,000 technology partners such as hospital information system (HIS) vendors, independent software vendors (ISVs), solution providers, service providers, systems integrators and every major global hardware manufacturer—are collaborating to meet the needs of healthcare IT.

Improving HIPAA and HITECH Compliance with vCloud for Healthcare

Using virtualization to consolidate servers, which in turn can eliminate hardware and reduce costs, is common practice for healthcare IT organizations transitioning to electronic records. With virtualization, healthcare IT can also easily move legacy applications to new platforms and support them with a robust management solution.

When assessing HIPAA compliance, auditors first look for evidence of scope assessment and validation for PHI. Consolidation may widen the scope, because hypervisors are put into consideration as just one of the guest systems handling PHI. Auditors also investigate access, seeking evidence of identity management and access control, including logs and monitoring. This process then typically leads auditors to review a list of incidents, logs and the subsequent actions. Neither HIPAA nor HITECH provide granular or prescriptive controls. Rather, they offer general rules to apply to configurations—whether deployments are on virtualized or physical infrastructure. Virtual infrastructure can be inherently more secure and stable than traditional physical infrastructure, making it easier for healthcare IT to isolate issues and avoid noncompliance penalties. Recent HIPAA enforcement actions have revealed that healthcare providers will benefit from monitoring access to PHI and from performing access authorization reviews and regular tests of access control gaps.

HIPAA divides controls into the following four areas that together have approximately 50 requirements (see Table 1):

- General rules
- Administrative safeguards
- Physical safeguards
- Technical safeguards

HIPAA SECURITY RULE	VMWARE CAPABILITIES TO ADDRESS THE RULE
§ 164.306 Security Standards: General Rules	Together with the industry-leading vSphere virtualization platform, vCloud for Healthcare helps to ensure the confidentiality, integrity and availability of ePHI that is created, received, maintained or transmitted. IT administrators can identify and prevent threats to the security or integrity of the information by performing sophisticated segmentation and monitoring of the virtual environment. Availability and integrity can be superior to physical environments because of unique virtualization capabilities such as systems snapshots, templates and VMware vSphere vMotion®.
§ 164.308 Administrative Safeguards	Virtualization and cloud technology can streamline regular and ongoing risk analysis, requiring fewer resources. By centralizing data and removing distributed storage, organizations can reduce threats to PHI. VDI provides end-user access to data without the need for a local copy. A cloud model can eliminate significant risk of removable storage loss—a primary cause of healthcare breach fines. Recovery from failure is also easier with virtualization snapshots and capabilities to copy and launch systems without downtime. VMware vCenter Configuration Manager™ provides a convenient review of how well security policies and procedures meet the security rule. Together, VMware and VMware security partners make access restriction to the "minimum necessary" possible with third-party software.

2 HIMSS Analytics. "Virtualization Software Market Share," 2013.

HIPAA SECURITY RULE	VMWARE CAPABILITIES TO ADDRESS THE RULE
§ 164.310 Physical Safeguards	Consolidation through virtualization reduces physical systems, which prevents physical server sprawl, removes legacy vendor lock-in, and reduces access risk. Using VDI and vCenter Configuration Manager for centralized policy management, IT can more easily control proper use of workstations and electronic media. Virtualization can practically eliminate the need for removable media by delivering simple yet advanced networking capabilities and system flexibility.
§ 164.312 Technical Safeguards	VMware has created advanced electronic network security measures to protect ePHI from being transmitted. With virtualization, healthcare IT has new control methods that can prevent ePHI from improper alteration or destruction—from copying and taking snapshots of virtual disks to using nonpersistent state. The software records access and other activities related to ePHI, and IT can easily examine them. Network and system monitoring, integration with identity management, and centralized orchestration enable only authorized individuals to access ePHI. Moreover, VMware VDI removes the requirement for all HIPAA-protected PHI to be encrypted on endpoints, because PHI resides in the data center, not on a desktop or laptop. This reduces the opportunity for breaches: if a device is lost or stolen, PHI data is not accessible.

Table 1. HIPAA Security Rules Addressed by vCloud for Healthcare

Implementing Four Key Recommendations by Using vCloud for Healthcare Technologies

VMware offers healthcare IT the following ways to comply more cost-effectively and easily with a growing number of government mandates and rapid changes related to PHI.

Establish a Trusted Zone for PHI

HIPAA and HITECH are clear about the importance of finding and managing PHI. The scope of protection must be documented and properly confirmed to reduce organizational risk, simplify compliance management, and control assessment costs. Within the IT environment, healthcare IT teams must be able to view the traffic between workloads. They need their critical applications and databases protected from threats that originate from less secure or unpatched systems, and they need to implement audit and compliance controls on in-scope hosts.

vCloud for Healthcare can greatly help healthcare IT scope protections. It includes VMware vCloud Networking and Security, which, unlike hardware-based alternatives, enables IT teams to create networks that scale with applications and to position security services exactly where they are needed. VXLAN creates highly scalable virtual networks that support any-to-any connectivity for load balancing, for VMware vSphere Fault Tolerance, and for vSphere vMotion—in almost any type of application architecture. Healthcare IT can create a network architecture that supports elastic allocation of compute resources across clusters or pods without physical network reconfiguration. As networks are virtualized, security, load balancing and other gateway services are fully aligned and integrated with the new paradigm to ensure maximum agility and utilization. Greater visibility into traffic flows enables easier policy creation, and IT teams can segment in-scope workloads for continuous compliance, maintaining trust zones for sensitive data.

With vCloud Networking and Security, healthcare IT can

- Easily segment applications from one another
- Enforce trust zones for all applications
- View and control network communications among virtual machines for instrumentation and compliance
- Implement agile policy enforcement

Moreover, several vCloud Networking and Security features make establishing a trusted zone for PHI easier than traditional methods. The hypervisor-level firewall in vCloud Networking and Security provides adaptive security that travels with virtual machines as they migrate from host to host. This enables enterprises to securely support their virtual applications in dynamic cloud environments. With vCloud Networking and Security, IT teams also can create trust zones that separate virtual machines with sensitive HIPAA data from other virtual machines.

vCloud Networking and Security includes an open architecture with industry-standard APIs to enable freedom of choice and avoid vendor lock-in. The solution provides service insertion at the virtual network interface card (vNIC) and the virtual edge level, which allows supported third-party products to access traffic flows and workload context without significant software development (see Figure 2). Now healthcare IT can easily take advantage of new technology, integrating operational workflows with existing systems and procedures. IT teams can also deploy consistent best-of-breed solutions across physical and virtual environments. With vCloud Networking and Security, healthcare IT can finally couple existing investments in networking and security solutions with virtualization, cloud efficiency and cloud agility.

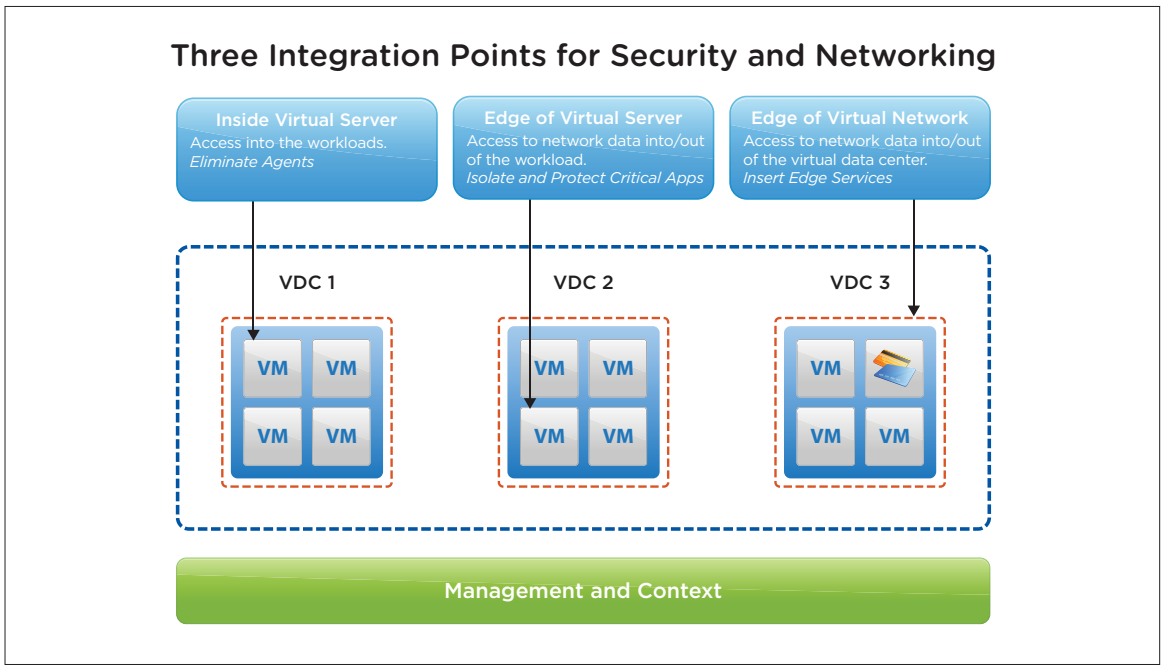

Figure 2. vCloud for Healthcare Security and Networking Integration Points

vCloud Networking and Security also enables granular and efficient access control in VDI environments, such as VMware Horizon View™. vCloud Networking and Security can be used to create logical security perimeters around individual virtual desktops or around the entire virtual desktop infrastructure. A HIPAA requirement, this capability ensures that VDI users can access only the applications and data they are authorized to use and also prevents unauthorized access into the broader virtual data center. Visibility into VDI traffic enables rapid troubleshooting and policy creation.

The benefits of using vCloud Networking and Security to secure virtual healthcare desktops include

- Better protection of virtual desktops from neighbor attacks
- More controlled access from virtual desktops to applications
- Improved isolation of the VDI environment from the rest of the virtual data center

Using vCloud for Healthcare, IT teams can automatically build a trusted zone for PHI data. Network isolation through Layer 3 firewall rules means a virtual environment can have a precise boundary set around PHI data, also isolating other systems that are out of scope. Establishing a trusted zone through both network perimeter and application-

level capabilities helps to segment traffic. The policy-aware trusted zone can be continuously validated, which means even a violation of policy (e.g., using vSphere vMotion over unsecured networks) can be detected and prevented. With scoping under control, healthcare IT is ready to assess technical and administrative controls (see Figures 3 and 4).

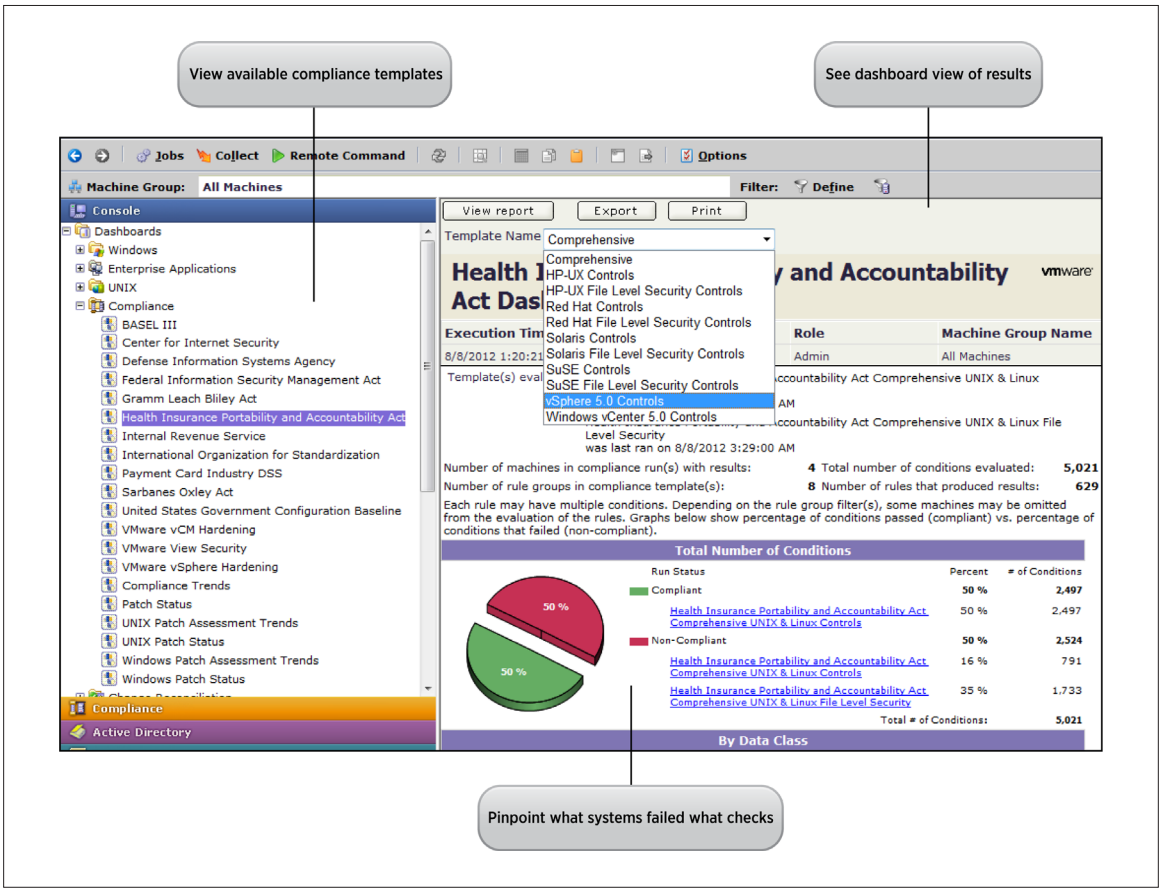

Figure 3. Improved Scope Assessment

Scan for Sensitive Data

HIPAA and HITECH compliance also requires healthcare IT to know where PHI exists. VMware vCenter™ Infrastructure Navigator™, also included in vCloud for Healthcare, determines which systems are sharing information and provides a simplified dashboard for understanding the complex relationships among applications. Together, vCloud Networking and Security and vCenter Infrastructure Navigator provide deep insight into the storage of sensitive data to identify communication streams and applications that depend on the data. They enable IT teams to discover and identify all workloads, dormant or active, to comply with the need to protect stored data.

In a virtual environment, scope assessment can be extremely thorough in scans for sensitive data. A virtual machine in a "powered-off" or suspended state is still visible in vCloud for Healthcare, which makes virtual systems scanning more transparent and effective than scanning physical-only systems. An environment considered out of scope also can be scanned more easily for sensitive information, further validating scope. vCloud Networking and Security makes it easier than ever for systems to be included, because if they are in vCloud for Healthcare, they already exist on an infrastructure that is capable of data loss prevention.

The dynamic nature of cloud environments means a data loss prevention service can also be extended and automated. An IT programmer can use APIs to automate controls—for example, creating a rule that automatically moves a virtual machine with sensitive patient data into the common desktop environment (CDE) and behind a firewall, or moves it into a lockdown zone pending investigation.

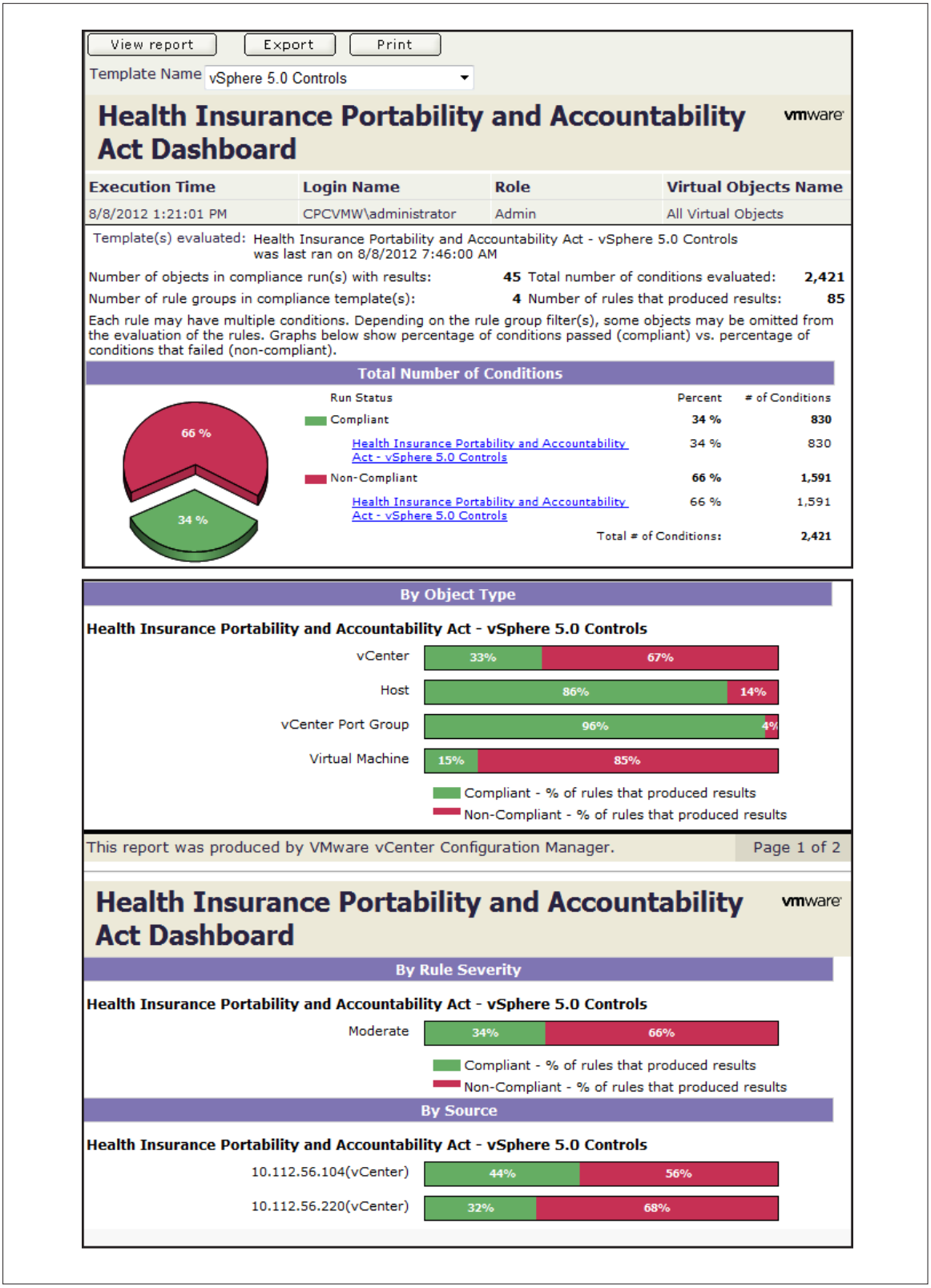

Figure 4. Compliance Results Dashboards

The flexibility and control offered in vCloud for Healthcare can simplify risk control when compared with physical-only environments. For example, how difficult would it be to isolate an out-of-compliance physical machine with network connectivity at the application level? With virtual machines, it is as simple as a rule. Now imagine a rule that requires a virtual machine with PHI to have network connectivity isolated at the application level (e.g., restrict certain protocols) and then send an email to administrators. A full assessment could push entire workloads and related systems with PHI data off a cluster that has insecure or out-of-scope systems to a cluster within a secure zone.

Enable Continuous Configuration Compliance

In patient-care environments, configuration management is an essential step to compliance. Detecting changes and keeping software up to date with the latest vendor recommendations are critical foundations for maintaining secure systems. With vCenter Configuration Manager, included in vCloud for Healthcare, IT teams can continuously and automatically monitor and patch infrastructure and applications. They can support detailed node discovery and assessment across both physical and virtual systems to centrally control changes and configuration. They can also inspect for HIPAA compliance, assess configurations against best practices and perform automatic remediation.

Using vCloud for Healthcare, IT can integrate vCenter Configuration Manager data with vCenter Infrastructure Navigator for passive and active probes to determine which assets constitute a service. Such probes can also map dependencies with details of protocols and networks.

Automation and data collection capabilities in vCenter Configuration Manager—such as the ability to perform assessments and work with guest systems (both Windows and Linux)—give administrators a broad view of the security and compliance status of the complete environment.

Rather than run through individual system settings to manually configure them, vCenter Configuration Manager performs a compliance assessment and generates a report with detailed rules and a pass-or-fail assessment. It identifies systems that aren't in lockdown mode, for example, and can help reveal unauthorized changes. Integration of vCenter Configuration Manager with existing operations-monitoring tools also enables operational or degradation issues in a virtual environment—for example, performance changes—to be correlated to a potential compliance violation. vCenter Configuration Manager has built-in guidelines for vendors, the Defense Information Systems Agency (DISA), the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS). The software also supports the NIST Security Content Automation Protocol (SCAP) to provide standardized yet detailed guidance of security configuration for operating systems and applications (see Figure 5).

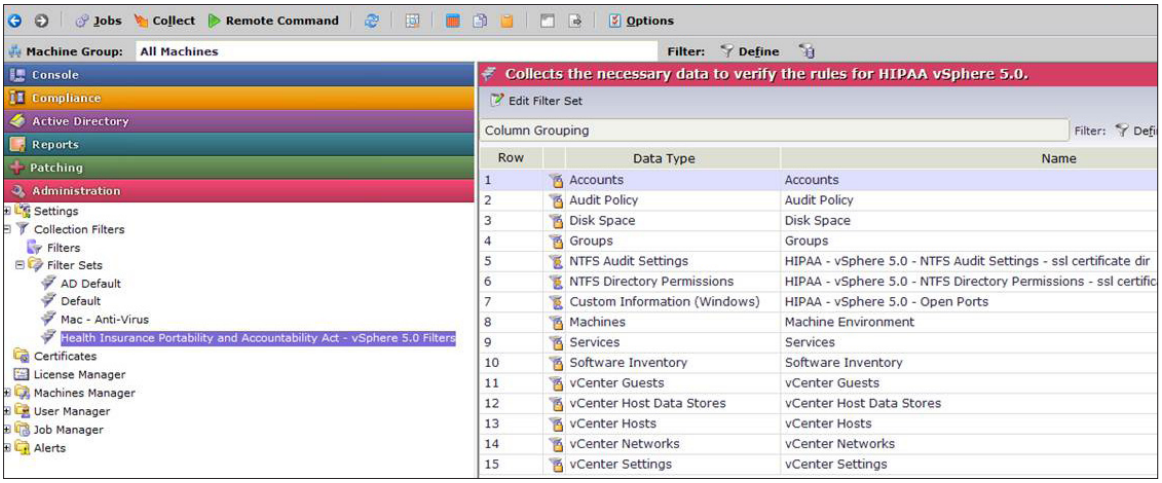

Figure 5. Simplified and Automated Configuration Management

Virtualization provides capabilities that surpass the continuous monitoring features of physical infrastructure. Virtualization enables IT to provision hundreds or even thousands of new virtual machines, knowing that a central system can track whether they all match a set of compliance requirements for a workload. Provisioning a guest can include hardening it dynamically so that virtual environments do not have to slow down to include manual compliance configuration and tests in the launch process. Furthermore, if any issues are found, vCenter Configuration Manager can bring virtual machines into conformance or work to isolate them. vCloud for Healthcare supports business process as well as infrastructure adjustment to more easily achieve continuous configuration compliance.

Remove Data From Endpoints to Prevent Data Theft or Loss

IT security auditors report that endpoint breaches—from lost or stolen laptops, desktop computers and storage devices—result in many HIPAA breaches, exposing hospitals to undue risk. Although healthcare IT teams want their busy clinicians to have better work-life balance through mobility, mistakes happen, and mobile devices or laptops containing PHI data are left in public areas, such as subways or restaurants. Whether the device is stolen or simply left by mistake, when PHI is handled by an unauthorized person, a HIPAA violation has occurred.

vCloud for Healthcare significantly reduces the threat of lost or stolen PHI, so hospital administrators know they are enabling clinician productivity without inviting HIPAA violations. A VDI solution built on Horizon View, AlwaysOn Point of Care delivers applications and data effectively and efficiently, yet all data remains in the data center. When end users log in to clinical applications—whether remotely or onsite—the experience is just like using a local application, but because information is being delivered from the data center in pixels, it cannot be stored or downloaded to the physical device or any external storage device. As a result, no data remains on a lost or stolen device, so no HIPAA violation occurs (see Figure 6).

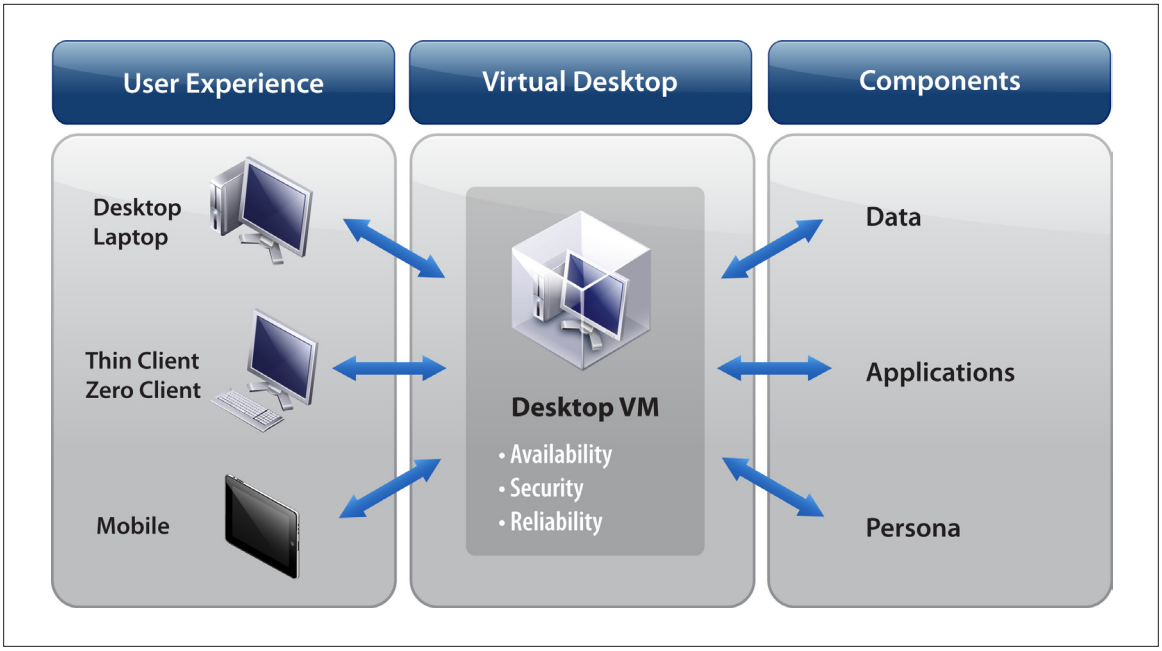

Figure 6. Maintaining Control of Data with vCloud for Healthcare

Checking Your Compliance and Contacting VMware

Because VMware understands how important yet complex it is to stay HIPAA- and HITECH-compliant, VMware has released a set of free compliance checkers for you to run in your hospital to assess the configuration compliance of your environment. These checkers can quickly alert you to areas of concern and help focus the efforts of your IT team as it considers the adoption and deployment of vCloud for Healthcare.

Regulated healthcare organizations can use vCloud for Healthcare to help reduce HIPAA and HITECH violations while helping to improve the cost, quality and delivery of patient care. vCloud for Healthcare enables healthcare IT to monitor access to PHI, perform access authorization reviews and regularly test for access control gaps. It also gives clinicians seamless and simple access to all applications, from any device, whether inside or outside the hospital. The only complete and integrated solution, vCloud for Healthcare delivers all of the components healthcare providers need to establish and operate a virtual, cloud environment while providing the necessary control and transparency to maintain compliance.

To learn more about vCloud for Healthcare for a compliant healthcare cloud or to access free VMware compliance checkers, please contact your VMware account executive today.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

 Item No: VMW-TWP-vCLOUD-FOR-HEALTHCARE-HIPAA-HITEC-USLET-104 02/13