HYTRUST
Cloud Under Control

A practical guide to HIPAA-compliant virtualization

White Paper

HYTRUST
Cloud Under Control

Table of Contents

4 Summary

4 Enforcement and virtualization increase the stakes

5 Privileged users complicate compliance

7 The platform is not a panacea

7 Solving the privileged user puzzle

9 Virtualize with compliance and con dence

10 Appendix A: HyTrust enables HIPAA security rule compliance
– Administrative safeguards: Section 164.308
– Administrative safeguards: Section 164.312

HYTRUST
Cloud Under Control

White Paper

A practical guide to HIPAA-compliant virtualization

"There's huge liability around the economics of HIPAA violations, the economics of breaches of personal health information. They're really daunting. We're talking multimillion dollar settlements on this stuff at this point."

Scott Lundstrom, Group VP,
IDC Health Data Insights, January 2012

"Security is not a one-time project, but rather an on-going, dynamic process that will create new challenges as covered entities' organizations and technologies change."

U.S. Dept. of HHS, HIPAA Security Series,
"Security 101 for Covered Entities"

"The governance and compliance challenges presented by virtualization are often overlooked in HIPAA risk assessments. While security breaches often surface due to administrative and technical control gaps, HyTrust is taking the right approach by imbedding automated controls to secure privileged access and accountability in the ePHI virtual environment."

Andrew Hicks,National Healthcare
Practice Lead, Coalfire Systems

Summary

Healthcare enterprises have achieved major cost savings, operational benefits, and great ROI from virtualizing lower tier workloads. However, many of these organizations are finding that further data center transformation presents new and daunting challenges. As a result, their virtualization initiatives are losing momentum, and some have been put on hold. The governance, security, and compliance needs of Tier 1 and 2 workloads are substantially greater than the needs of less critical applications, and the base virtualization platform is not designed to meet those needs.

This paper will provide guidance on overcoming the challenges of HIPAA compliance in virtualized data centers and accelerating returns on virtualization investments with access policy enforcement from HyTrust.

Enforcement and virtualization increase the stakes

HIPAA compliance ain't what it used to be.

For the first 10 years of its existence, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was a toothless tiger. Covered entities were given years to prepare for the 2005 compliance deadline. For several years thereafter, the Department of Health and Human Services' Office of Civil Rights (OCR) assessed almost no significant civil fines despite thousands of consumer complaints. Even if OCR had been inclined to prosecute non-compliance, the cap on negligent violations of the law ($25,000 per year) made non-compliance a low cost option for mid-size and large healthcare enterprises.

The situation changed dramatically in 2009 with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The law both raised the ceiling on HIPAA civil penalties by a factor of 60X - up to $1.5 million per calendar year for "willful neglect" of a single provision - and mandated aggressive prosecution of HIPAA violations. Since passage of the HITECH Act, OCR has reached non-compliance settlements of $1 million or more with covered entities on multiple occasions. Almost overnight, HIPAA went from a low priority to a "must do" for most healthcare organizations.

HYTRUST
Cloud Under Control

10 key risks to virtualization and compliance

- Hypervisor environment is in scope
- One function per server
- Separation of duty
- Mixing VM's of different trust levels
- Dormant VMs and VM snapshots
- Immaturity of monitoring solutions
- Information leakage
- Defense in depth
- VM Hardening
- Cloud Computing

For IT management in covered entities, the challenges of compliance with HIPAA are compounded by accelerating technological change. Virtualization is revolutionizing IT operations due to its compelling financial and operational benefits. Analysts estimate that about half of all data center workloads now run in virtual machines. Virtualization's cousin – cloud computing – is in an earlier phase of adoption, but it promises to have a similarly profound impact on IT infrastructure.

Rapid technological change makes compliance with the IT security-related requirements of the HIPAA Security Rule and HITECH a moving target. Many IT organizations are only beginning to understand that virtualization has attributes that traditional security and compliance measures don't account for. They're also discovering that the baseline security functionality of the VMware platform, while usually sufficient for lower tier, non-compliance workloads such as software development and testing, was not designed to fulfill the stringent requirements for securing electronic protected health information (ePHI).

Large healthcare organizations have responded to these challenges in two main ways. Some have slowed or postponed virtualizing workloads with ePHI rather than risk a costly breach or compliance penalty. By doing so, they're passing up the substantial increase in ROI and other economic benefits available from greater virtualization.

Other covered entities are virtualizing workloads with ePHI, despite the risks. Most aren't fully aware of the compliance issues; others understand the risks but have postponed dealing with them. These enterprises are paying for increased virtualization benefits with an increased risk of security breaches and large, government-imposed penalties.

Privileged users complicate compliance

Subpart §164.306 of HIPAA, "Security standards: General rules", states that covered entities must:

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 the HIPAA Privacy Rule.

4. Ensure compliance by its workforce

All four requirements involve ensuring compliant behavior by "privileged users". In a VMware environment, these are the vCenter users who have administrative rights allowing them to make major changes to most elements of the virtual infrastructure. Privileged users may include non-IT employees, contractors, consultants, or external partners in addition to the enterprise's own VMware admins. They have the "keys to the kingdom" due to the exceptionally wide range of capabilities and freedoms the vSphere platform gives them. With a few mouse clicks, they can:

- Create and delete virtual machines (VMs) that process ePHI

- Power up and power down production VMs and virtual security appliances

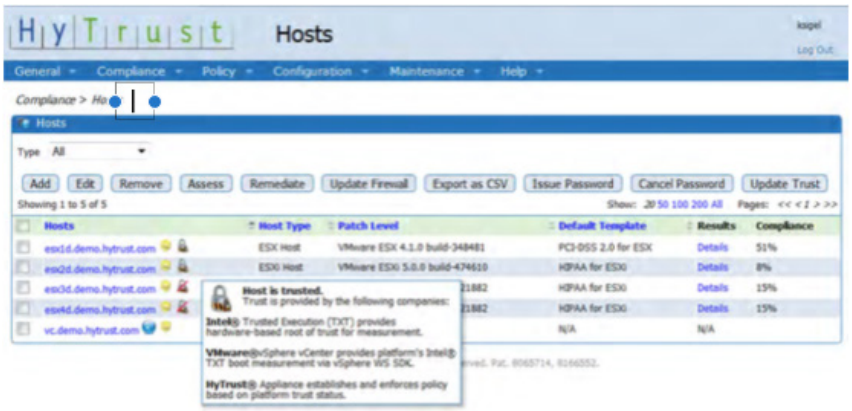
- Make copies of VM images containing ePHI
- Reconfigure virtual network interfaces and move VMs across virtual network segments and trust zones
- Bypass admin logging mechanisms by connecting directly to ESX/ESXi hosts
- Share root passwords, eliminating the enterprise's ability to link a particular operation or request to an individual user

Clearly, any list of "reasonably anticipated threats ... or disclosures" includes the possibility of a privileged user misusing ePHI, unintentionally or intentionally. A PricewaterhouseCoopers/Wall Street Journal study in April, 2012, found that 56 percent of respondents who said they had experienced economic crime in the past 12 months said the main perpetrator of the most serious fraud was someone inside the organization.[1]

Many HIPAA requirements involve procedures for authorizing privileged users or logging privileged user actions.

1. "Ensure that all members of [the] workforce have appropriate access to ePHI"
2. "Protect the ePHI of the clearinghouse from unauthorized access by the larger organization"
3. "Implement procedures for monitoring log-in attempts"
4. Implement procedures for information systems that "allow access only to those persons or software programs that have been granted access rights"
5. "Assign a unique name and/or number for identifying and tracking user identity"
6. Implement "mechanisms that record and examine activity in information systems that contain or use ePHI."
7. "Implement policies and procedures to protect ePHI from improper alteration or destruction."

Some of these requirements apply to non-privileged as well as privileged users. However, a covered entity may have established compliance for its non-privileged users without fully addressing the same requirements for VMware privileged users. It may also have secured the VM guest operating system but not the underlying virtual infrastructure.



Graphic illustrates HyTrust Appliance verifying trusted host by Intel, VMware, and HyTrust. Graphic also shows percent compliance against HyTrust compliance templates

[1] http://online.wsj.com/article/SB10001424052970203753704577255723326557672.html

Mitigating the compliance risks associated with privileged users involves applying such time-honored principles as separation of duties, least privilege, and access policy enforcement. This is no small feat in the physical data center, but in the virtual environment it has been a major barrier to virtualizing workloads with ePHI.

The platform is not a panacea

IT professionals sometimes assume that the VMware platform itself provides sufficient ePHI protection for HIPAA compliance. After all, virtualization technology brilliantly achieves its goals of improving data center performance, efficiency, agility, and survivability. However, security and compliance depend on different technologies and expertise, and the developers of the virtualization platform have focused on their core mission rather than those other domains.

The minimal emphasis on security had little impact during the early years of virtualization adoption. The non-critical workloads that were virtualized – development and testing, for example – were adequately served by the platform's basic security measures. As enterprises moved toward virtualizing mission critical applications that process sensitive data such as ePHI, they began discovering that the VMware infrastructure does not offer all the functionality needed for compliance with HIPAA and other regulations. This is especially true in the area of privileged user management :

Examples of gaps include:

- Lack of enterprise-class enforcement of privileged user policies
- Limited role-based access controls (RBAC) that are rarely granular enough to enable least privilege permissions and separation of duties
- Maintenance-oriented logs that include only some of the data required for compliance and cover only some administrative access methods
- Lack of automated host log data aggregation

It's no wonder that many healthcare enterprises slowed or stopped virtualizing their ePHI applications.

Solving the privileged user puzzle

The key to HIPAA compliance for ePHI workloads is to apply the same types of compensating controls used in the physical data center to the virtual environment, while accounting for the unique aspects of virtualization. That's why HyTrust developed a solution purpose-built for enforcing privileged user policies in the virtualized environment. With HyTrust, covered entities can now meet the administration-related requirements of HIPAA, mitigate the risk of ePHI exposure, and extend the economic benefits of virtualization.

HyTrust secures the virtual infrastructure and supports HIPAA compliance with:

1. Fine grained authorization that enables least privilege and separation of duties by enforcing both role- and asset-based access policies. HyTrust's asset-based controls limit access to specified VMs or other virtual resources, an essential requirement for isolating workloads in multi-tenant environments and/or collapsed application tiers for better compute utilization

HYTRUST
Cloud Under Control

"Proactive control of user permissions is a 'must have' for a secure next generation data center."

It's equally important that access controls for the virtualized environment be transparent to and efficient for the general user which HyTrust delivers."

Patrick Enyart
Enterprise IT Security, McKesson

2. Audit-quality logging that automatically aggregates comprehensive, user-specific log data on every attempted user request, including the change operation

3. Strong, multi-factor authentication of the user for access to the virtualization platform that prevents unauthorized access due to password cracking or theft.

4. Infrastructure integrity based on automating hypervisor configuration hardening, remediation, and policy compliance.

The HyTrust Appliance, which is a virtual appliance, sits logically between privileged users and all points of access to VMware infrastructure administration. This allows HyTrust Appliance to log every attempted administrative operation and consistently enforce enterprise-defined access policies. HyTrust prevents host root password sharing and default password usage, so all privileged user activity is associated with a unique ID (necessary for complying with HIPAA requirement 164.312 (a)(2)(i)).

To address requirement 164.312 (b) and support forensic analysis, HyTrust Appliance logs standard compliance data that is very difficult or impossible to get from the VMware platform. Examples include denied and failed user requests, source IP addresses, and resource reconfiguration details.

While both HyTrust Appliance and the virtualization platform integrate with Microsoft Active Directory (or any LDAPv3 compliant directory), HyTrust Appliance access policies enable much more specific role definitions. HyTrust Appliance policies are based on command-level permissions which are consistent across all methods of accessing VMware infrastructure. They are also able to restrict users further by defining the IP address range and/or access method they can come from and use. This degree of specificity is needed to segregate the duties of many different types of privileged users without compromising either productivity or compliance with HIPAA requirements such as 164.308 (a)(3)(i).

Healthcare organizations can opt to use HyTrust's exclusive secondary approval workflow for greater flexibility in protecting EPHI. When a VMware user attempts a specified operation involving protected information, HyTrust Appliance can automatically seek higher-level authorization before it allows the user to execute the operation. Secondary approval can assure that high consequence actions such as snapshotting a VM only occur when they comply with HIPAA requirements.

HyTrust Appliance's asset-based access controls also play a key role in current and future HIPAA compliance. As server consolidation ratios increase and multi-tenancy in private clouds becomes more common, data centers need to isolate each tenant's

workloads without physical air-gapping. HyTrust Appliance isolates EPHI workloads by enforcing access and infrastructure segregation policies on individual VMs and other virtualized resources such as hosts, networks, resource pools, and more. For instance, it can ensure that privileged users who lack authorization to access EPHI cannot move a VM that handles patient information to a non-HIPAA compliant network segment. This HyTrust Appliance capability directly addresses HIPAA requirement 164.308 (a)(4)(ii)(A).

A complete mapping of HyTrust Appliance functionality to specific HIPAA requirements is presented in the appendix of this document.

In addition to enabling regulatory compliance, HyTrust Appliance provides valuable operational benefits. For example, virtualization teams can now confidently increase self-service by the growing number of non-IT privileged users. These users can be given the minimal level of access to the virtual infrastructure they need to do their jobs, while VMware administrators reclaim time for more valuable, higher skilled work.

Virtualize with compliance and confidence

The financial and operational benefits of virtualizing more of the data center have grown very large, but so have the potential penalties for overlooking the impact on HIPAA compliance. Effective governance of the virtual infrastructure is as critical as governance of the physical data center; patient information must be protected equally well in both environments. The VMware platform wasn't designed to fulfill all of HIPAA's requirements for controlling access to ePHI, so relying on it alone for compliance can be a high risk, high reward proposition.

HyTrust Appliance enables healthcare enterprises to achieve the virtualizing EPHI workloads, without the high risk. It enforces policies that deliver the least privilege access, separation of duties, audit-quality log data, and effective governance of privileged users that HIPAA compliance in the virtualized environment requires. For additional product information visit http://www.hytrust.com/products/capabilities, email questions to hipaa@hytrust.com, or call (sales 650-681-8100) for a free consultation.

HyTrust - Cloud Under Control.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100

HYTRUST
Cloud Under Control

Appendix A:
HyTrust enables HIPAA security rule compliance

The regulations that implement the security provisions of HIPAA are titled "Security Standards for the Protection of Electronic Protected Health Information" but are more commonly known as the Security Rule. The standards are divided into the categories of administrative, physical, and technical safeguards. In the virtualized data center, HyTrust safeguards enable compliance with most HIPAA administrative and technical standards.

HYTRUST
Cloud Under Control

Administrative safeguards: Section 164.308

Sub part	Implementation specifications	Virtualization platform constraints	HyTrust compliance support
164.308 (a)(l)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain, and correct security.	Inadequate support for privileged user risk analysis, limited ability to manage privileged user risk, and inadequate support for privileged user sanctions	Provides thorough support for risk analysis, risk management, and user sanctions in the virtual environment
164.308 (a)(l)(ii)(A)	Risk analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI help by the covered entity.	Incomplete, multi-format, and non-user specific logs of privileged user activity prevent an accurate and thorough assessment of risks to ePHI	Provides complete, standardized, and user-specific logs of privileged user activity enables an accurate and thorough assessment of risks to ePHI
164.308 (a)(l)(ii)(B)	Risk management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).	Not designed to fully "protect against any reasonably anticipated uses or disclosures of such information" (164.306(a)(3)) by privileged users	Purpose-built to fully protect against any reasonably anticipated use of data by privileged users in virtual environments, by enforcing fine-grained access policies and requiring secondary approval of user actions, as desired
164.308 (a)(l)(ii)(C)	Sanction policy (R): Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.	Incomplete documentation of privileged user activity may limit ability to apply sanctions due to legal concerns	Provides thorough documentation of privileged user activity, enabling ability to apply sanctions without legal concerns
164.308 (a)(l)(ii)(D)	Information system activity review (R): Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Incomplete logging of unique user IDs, access methods, and operations such as denied requests prevents effective review of privileged user activity	Provides thorough logging of unique user IDs, all access methods and operations, and secondary approval decisions, enabling effective review of privileged user activity
164.308 (a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to ePHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to ePHI.	Inadequate ability to define and enforce least privilege access control policies customized to the very specific needs of all types of privileged user roles in virtual infrastructure	Enables definition and enforcement of detailed, highly customizable least privilege policies tied to the specific needs of all types of privileged user roles in the virtual infrastructure
164.308 (a)(3)(ii)(A)	Authorization and/or supervision (A): Implement procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Incomplete logging of unique user IDs, access methods, and operations such as denied requests prevents effective supervision of privileged user interactions with VMs holding ePHI No efficient way to authorize or deny specific user requests	Provides thorough logging of unique user IDs, all access methods, and all operations, enabling effective supervision of privileged user interactions with VMs holding ePHI. Offers automated secondary approval of users requests to aid supervision.
164.308 (a)(4)(i)	**Information access management:** Implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of subpart E of this part.	Limited ability to enforce separation of duties and least privilege access to ePHI	Enforces highly customizable policies that provide separation of duties and least privilege access to ePHI

HYTRUST
Cloud Under Control

Administrative safeguards: Section 164.308 (Cont.)

Sub part	Implementation specifications	Virtualization platform constraints	HyTrust compliance support
164.308 (a)(4) (ii)(A)	Isolating healthcare clearinghouse functions (R): If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization	Provides broad RBAC not customized to the specific needs of all "internal customers" of the virtual infrastructure Does not isolate segments of the virtual network from unauthorized users	Enables definition and enforcement of detailed, highly customizable RBAC tied to the specific needs of all "internal customers" of the virtual infrastructure Isolates segments of the virtual network from unauthorized users
164.308 (a)(4)(ii)(B)	Access authorization (A): Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism	Inadequate ability to enforce policies customized to different privileged users' need to access virtual infrastructure management tools	Enables enforcement of policies customized to level of access different privileged users need via secondary approval and root password vaulting Officers automated workflow for requiring secondary approval of user actions, and root password vaulting for granting privileges for specialized requests
164.308 (a)(4) (ii)(C)	Access establishment and modification (A): Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process	Limited ability to make targeted modifications to a role's right of access to virtual infrastructure management tools, based on authorization policies	Enables very targeted modifications to a role's right of access to virtual infrastructure management tools, based on authorization policies and secondary approval rules
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents.	Potential privileged user anonymity	Every virtual infrastructure operation linked to a specific privileged user in log data
164.308 (a)(6)(ii)	Response and reporting (R): Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Incomplete, possibly non-user specific log data prevents effective incident detection, response, and documentation	Provides the thorough, user-specific log data needed for effective incident detection, response, and documentation
164.308 (a)(8)	**Evaluation:** Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of ePHI that establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Incomplete, possibly non-user specific log data prevents effective auditing of access control policies and procedures designed to protect ePHI	Provides the thorough, user-specific log data needed for effective auditing of access control policies, procedures, and secondary approvals designed to protect ePHI

HYTRUST
Cloud Under Control

Administrative safeguards: Section 164.312

Sub part	Implementation specifications	Virtualization platform constraints	HyTrust compliance support
164.312 (a)(l)	**Access control:** Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4)	Potential privileged user anonymity, in addition to overly general RBAC	Links every virtual infrastructure operation to an specific privileged user in log data, while enforcing RBAC that ensure least privilege access to ePHI
164.312 (a)(2)(i)	Unique user Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	Share root access by privileged users prevents tracking each user's activity in the virtual environment	Ensures all activity in the virtual environment is tied to a specific privileged user's ID in log data
164.312 (b)	**Audit controls:** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Does not capture critical log data (denied operations), source IP, resource reconfiguration details, etc.), and potentially records non-user specific activity Creates separate log files for vCenter and each host, and uses different log formats for vCenter vs. hosts	Capture all essential log data with a unique user ID for all activity Records all relevant details of secondary approval workflow Consolidates and centrally manages logs covering vCenter and all hosts, in a uniform format Records all changes to access and hardening policies as well as results of all hypervisor hardening assessments and remediations
164.312 (c)(l)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Inadequate ability to ensure a VM with ePHI is not deleted	Ensures VMs with ePHI aren't deleted, based on both RBAC and asset-based access controls
164.312 (c)(2)	Mechanism to authenticate electronic protected health information (A): Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	Shared root access by privileged users can make it impossible to distinguish between authorized and unauthorized changes to VMs with ePHI	By logging each privileged user's activity, provides an audit trail of unauthorized alteration or destruction of any VM with ePHI, ensuring accountability
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Single factor (password) authentication may be breached if user password is weak or stolen	Adds multi-factor authentication support to the virtualization platform (via RSA SecurID or CA ArcotID), mitigating the risk of unauthorized access

Note: Standards and implementation specifications not addressed by HyTrust have been omitted from the tables.