HYTRUST
Cloud Under Control

Solution Brief

Can you be HIPAA/ HITECH compliant in the cloud?

Summary

- As more organizations virtualize their clinical and ePHI applications, their virtual servers must now be brought into compliance with HIPAA/HITECH
- The native capabilities in virtualization platforms such as VMware vSphere are not suf cient to meet all HIPAA/ HITECH control requirements
- HyTrust CloudControl™ and HyTrust DataControl™ support a total of five HIPAA controls in the areas of hypervisor administration and data at rest encryption
- DataControl encryption also supports the HITECH Safe Harbor provision to protect the organization from the breach noti cation requirement in case of lost ePHI
- HyTrust lowers the cost of HIPAA compliance by enabling mixed-mode deployments and supporting lower audit sampling level requirements

Background

For the first 10 years of its existence, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was a toothless tiger. Although in theory compliance was required by 2005, many organizations ignored HIPAA even beyond that date because audit enforcement and potential fines were extremely low.

The situation changed dramatically in 2009 with the passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The law 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), mandated aggressive prosecution of HIPAA violations, and implemented a breach notification requirement. Since passage of the HITECH Act, the Department of Health and Human Services has reached non-compliance settlements of $1 million or more with covered entities on multiple occasions. Even more damaging, any loss of over 500 health records forces public disclosure of the breach, causing loss of reputation and customer trust. Almost overnight, HIPAA went from a low priority to a 'must have' for most healthcare organizations.

Rapid technological change makes compliance with the IT security mandates of the HIPAA and HITECH a moving target. Many IT organizations are only beginning to understand that virtualization has implications that traditional security and compliance measures don't account for. They're discovering that the security and audit features of the VMware platform, while usually sufficient for lower tier, non-compliance-oriented applications like test and dev, were not designed to meet the stringent requirements for securing electronic protected health information (ePHI).

The hypervisor and HIPAA compliance

All interpretations of HIPAA agree that in order to secure ePHI, the platforms that host ePHI must be compliant as well. As organizations adopt virtualization as a mainstream, default platform, the need for compliance controls on VMware vSphere in particular is mandatory.

IT professionals sometimes assume that the VMware platform itself provides sufficient ePHI protection for HIPAA compliance. After all, vSphere brilliantly achieves its goals of improving data center performance, efficiency, agility, and survivability. However, security and compliance depend on different technologies and expertise, and VMware has chosen to focus in other areas, leaving significant gaps with

respect to compliance controls. This is especially true in the area of privileged user management, where the following gaps exist:

- Lack of enterprise-class strong authentication of privileged user accounts
- Limited role-based access controls (RBAC) that are granular enough to enable least privilege permissions and separation of duties
- Insufficient log detail and event coverage for compliance reporting
- vSphere also lacks an encryption solution for data at rest security, as well as a native option for hardening the hypervisor configuration. Both are required in almost all compliance regimens, including HIPAA

HyTrust control support for HIPAA

The key to HIPAA compliance for ePHI workloads is to apply the same types of controls used in the physical data center to the virtual environment, while accounting for the unique aspects of virtualization. HyTrust support for HIPAA is delivered in two solutions: Hytrust CloudControlTM for privileged user controls, and Hytrust DataControlTM for encryption.

HyTrust CloudControl software is purpose-built to ensure that privileged administrators managing the virtual enviroment meet the security requirements of HIPAA, while mitigating the risk of ePHI exposure and extending the economic benefits of virtualization. HyTrust secures the virtual infrastructure and supports HIPAA compliance with:

- Strong, multi-factor authentication of the administrator access to vCenter and vSphere that prevents unauthorized access due to password cracking or theft
- Fine graining 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
- Audit-quality logging that automatically aggregates comprehensive, user-specific log data on all administrative activity. This eliminates the control gaps created by the limited native VMware logging
- Infrastructure integrity based on automated hypervisor configuration hardening, remediation, and policy compliance using pre-defined templates for HIPAA

It is important to note in particular the need for controls on the hypervisor administrator. It is not uncommon for a covered entity to have established access control 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.

HyTrust DataControlTM, on the other hand, delivers data-at-rest encryption for Windows and Linux workloads. The solution supports both public and private cloud with unified key management controlled by the covered entity. Encryption is a critical control for not just HIPAA itself, but to also prevent compromised ePHI from being declared "lost", thereby triggering the breach notification requirement.

Both CloudControl and DataControl functions directly map to a number of HIPAA/HITECH controls. See Appendix 1 for more detail.

Lowering the cost of HIPAA compliance

Healthcare organizations are continuously striving to deploy IT resources more efficiently. HyTrust supports this goal by lowering the cost of HIPAA compliance in two ways: mixed mode virtualization and control sampling:

Mixed Mode Virtualization - Many firms are mixing HIPAA and non-HIPAA workloads on the same virtual infrastructure, in order to lower cost and operational overhead. However this "mixed mode" deployment model creates compliance challenges, because it's much more difficult to segment in-scope user and administration activity from the non-HIPAA workload administration. HyTrust CloudControl makes this much easier by supporting role-based access controls on the admins, allowing the HIPAA workloads to only be touched by specific people. Furthermore, DataControl supports assigning keys for storage encryption based on specific workload policies, which means that the HIPAA virtual servers can be encrypted with dedicated keys that are not used for any other purpose.

Control Sampling - Like all audits, HIPAA audits rely on sampling to determine if a given set of controls were active over the period in question. If automated systems are used to implement controls, auditors will usually require less sampling, since automated controls are much more likely to be reliably operationalized. This also helps lower the cost and effort of the audit and provides support that the test data for the audit will be simple to obtain.

Summary

The financial and operational benefits of data center virtualization are significant, but so are the financial and reputational penalties for HIPAA non-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 HIPAA's requirements for securing ePHI, so relying on it alone for compliance is not a realistic option.

HyTrust CloudControl and DataControl enable healthcare covered entities to virtualize ePHI workloads and still meet HIPAA/HITECH requirements. They enforce controls for strong authentication, separation of duties, audit-quality logging, configuration hardening, and data at rest encryption. Together they enable operationally efficient compliance and data protection for healthcare organizations of all sizes.

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 1: Hytrust CloudControl and HyTrust DataControl HIPAA support details

CloudControl (CC) and DataControl (DC) support the following HIPAA Administrative and Technical Safeguards.

Administrative Safeguards	HyTrust Support
164.308 (a)(1)(ii)(D): Information System Activity Review	CC: Detailed audit log of all virtualization administration activity
164.308 (a)(3)(i): Workforce Security	CC: Strong authentication and authorization of virtualization administration DC: Encryption of data volumes containing ePHI
HITECH Breach Noti cation Requirement	DC: Safe Harbor Encryption: Data is made "unusable, unreadable, or indecipherable to unauthorized individuals"

Technical Safeguards	HyTrust Support
164.312(a): Access Controls	CC: Strong access controls and segregation of duties on administrators; DataControl (DC): Encryption of data at rest as required in 164.312 (a) (2) (iv); DC: compensating control to protect data at rest from access
164.312(b): Audit Controls	CC: Strong audit controls on hypervisor admins
164.312(c): Integrity Controls	DC: Encryption of data at rest to prevent modi cation of data that bypasses application or access controls
164.312(d): Authentication Veri cation	CC: Strong (2-factor) Authentication of hypervisor admins
164.312(e): Transmission Security	DC: Encryption of volumes being transmitted