HIPAA/HITECH Compliance Using VMware vCloud Air

Last Updated: September 23, 2014

WHITE PAPER

vmware®

Introduction

This paper is intended for security, privacy, and compliance officers whose organizations must comply with the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, and others responsible for maintaining compliance with those Acts.

HIPAA and HITECH establish rules covering healthcare organizations and their business associates to assure the privacy and security of Protected Health Information (PHI), including PHI contained in Electronic Medical Records (EMR). When such an organization entrusts PHI to a business associate for processing or storage, for example in a Cloud Service, responsibility for compliance with HIPAA and HITECH rules may fall to the organization or its associate, or it may become a joint responsibility of the organization and its associate.

The paper:

- **Outlines individual and joint responsibilities** of VMware clients who must comply with HIPAA and HITECH rules, and VMware as their business associate, when PHI is transmitted to, stored in, processed by, and retrieved from VMware vCloud® Air™.
- **Introduces the VMware Business Associate Agreement** documenting VMware's commitment to use appropriate privacy and security safeguards against unauthorized use or disclosure of PHI, and to respond appropriately to data breaches.

Responsibilities for Protected Health Information in the Cloud

Healthcare providers, insurers, and other organizations comply with HIPAA and HITECH rules by instituting, documenting, and auditing processes to assure the privacy and security of patients' Protected Health Information. Technologies like Cloud computing can't themselves be HIPAA-compliant or noncompliant, but technology providers' practices become part of the compliance discussion when they affect PHI privacy and security.

VMware has developed an information security management program for its vCloud Air, incorporating essential elements of HIPAA and HITECH. But healthcare and insurance clients must understand the limits of VMware's—or any Cloud Service Provider's—control over the components and processes of cloud computing. Understanding these limits will help VMware and its clients define their roles and responsibilities logically, so that they can meet their individual and joint privacy and security obligations without duplication or gaps.

Individual Responsibilities and Limits to Control

Organizations are responsible only for processes they control. For instance, VMware maintains the infrastructure that stores information sent or created by vCloud Air tenants as "virtual machines", "virtual disks", etc., on vCloud infrastructure. VMware maintains and controls the data centers, physical infrastructure, and management systems that make up this infrastructure, and is therefore responsible for elements associated with the infrastructure, including for example:

- **Administrative safeguards** – policies and procedures governing access controls, incident response, backup and recovery, etc.
- **Physical safeguards** – infrastructure, policies, logs, records, and procedures to control physical access to PHI and guide its secure disposal.
- **Technical safeguards** – access controls for electronic communications containing PHI, including encryption and network security associated with the infrastructure, but not tenant systems or data.

VMware also controls, and is responsible for, the processes by which it notifies Service tenants following discovery of a breach of unsecured PHI.

But VMware cannot control the way the information is represented, stored, or protected by vCloud Air tenants within their virtual machines, disks, etc., running or stored on the Service or traveling across networks over which tenants have administrative control. For example, VMware cannot determine or maintain the integrity of:

- **Client operating systems or applications** they contain (security, intrusion prevention, patch management, etc.).
- **Client and public networks** over which information travels to, from, or within a tenant's vCloud Air subscription.
- **Policies** by which its clients information from being read by third parties (encryption), grant access to PHI (authorization), make sure only authorized individuals access it (authentication), protect it from being read by third parties (encryption), and so on.

Clients are individually responsible for assuring compliance of these and other processes under their control.

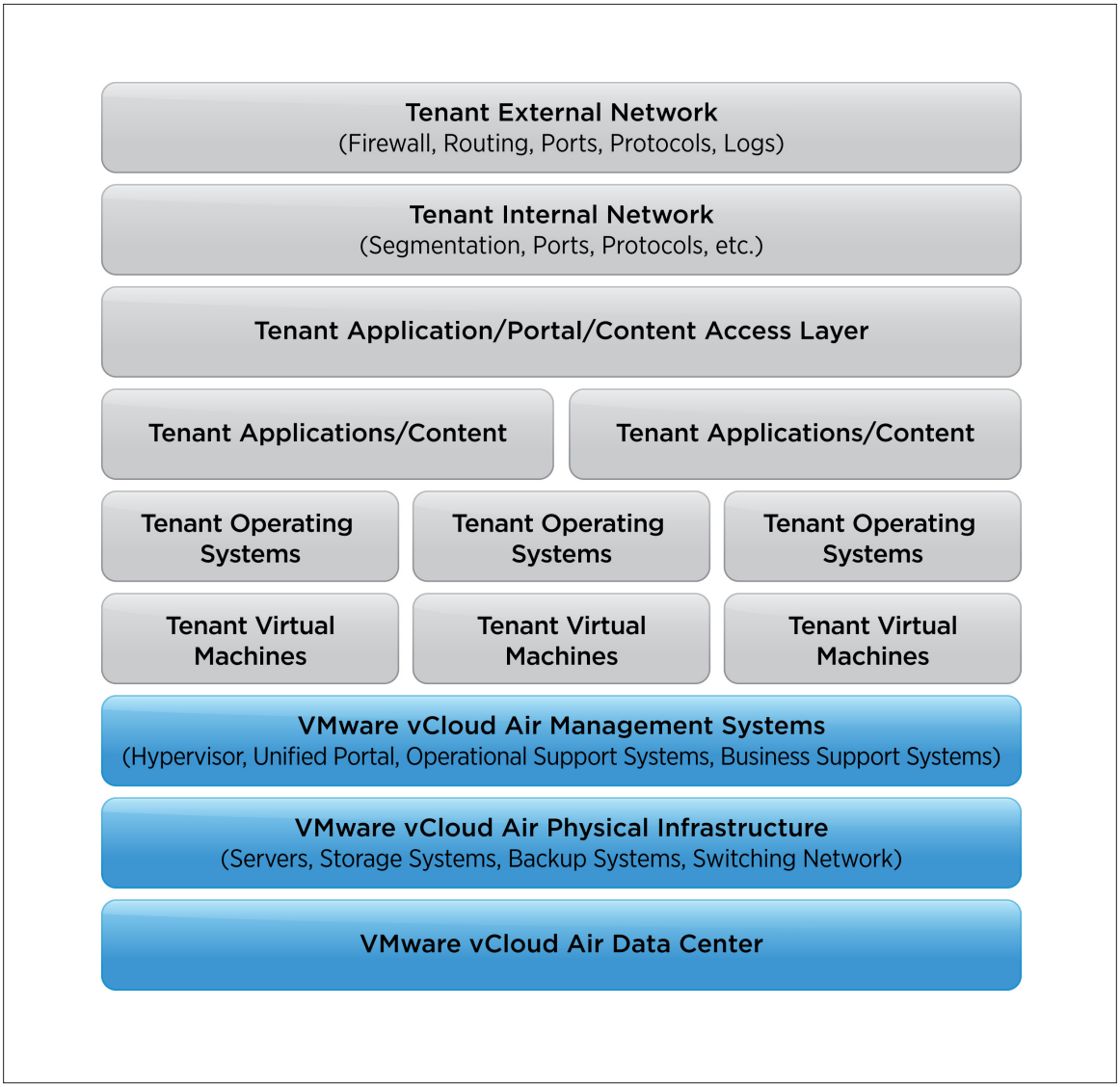

Figure 1. This "Responsibility Stack", illustrates the limits of control and areas of individual responsibility for VMware and tenants of its vCloud Air.

Joint Responsibilities

Not every HIPAA/HITECH requirement is the exclusive responsibility of one party or another. VMware vCloud Air offers many services that, when adopted and properly applied by a Service tenant, can help them maintain HIPAA- and HITECH-compliance of their processes. In these cases, VMware is responsible to meet its contractual obligations to Service tenants, and tenants are responsible to adopt and use the services as needed to meet their obligations. These are some examples of joint responsibilities:

- **Access Controls** – VMware provides a means to deny unauthorized persons access to vCloud Air; tenants manage user accounts to keep authorizations up to date, delete accounts when users leave the organization, etc.
- **Firewall** – VMware logically segregates the virtual systems of vCloud Air tenants and provides technologies to secure communications among tenant's virtual machines and data centers. Tenants document, implement, and test their instances of these technologies to assure the security of PHI in their care.
- **Disaster Recovery** – VMware documents, implements, and regularly tests business continuity and disaster recovery plans; tenants document and implement their own such plans and assure that PHI in their care is recoverable.

Overall, organizations required to comply with HIPAA and HITECH rules are responsible to adopt and use VMware vCloud Air in a manner that achieves and maintains that compliance.

VMware Business Associate Agreement

VMware is committed to serving the healthcare market with a broad range of reliable, high-performance Cloud Computing services. To help VMware vCloud Air clients document their compliance with HIPAA and HITECH rules, we provide a Business Associate Agreement that documents VMware's contractual obligation to use appropriate safeguards to:

- **Prevent** unauthorized access, use, or disclosure of Protected Health Information
- **Respond** to data breaches quickly and appropriately

Current or potential clients interested in reviewing the Business Associate Agreement should contact their VMware representative for full details.

Disclaimer

This paper is not intended as legal advice. Clients should consult qualified legal and compliance advisers when making decisions about HIPAA/HITECH compliance and the use of VMware vCloud Air. VMware neither expresses nor implies any warranty about the accuracy or fitness for any purpose of the information in this document.

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-HIPAA-HITECH-COMPLIANCE-USING-VCLOUD-AIR-USLET-101 09/14