Table of Contents

Introduction........................................................................................................................................2
Responsibilities for Protected Health Information in the Cloud .........................................................2
Joint Responsibilities...........................................................................................................................5
VMware Business Associate Agreement .............................................................................................5
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.

This 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 Horizon® 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.

• **Discusses the security posture** and measures in place for our Horizon Air product.

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
Horizon 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 Horizon Air tenants as “virtual machines”, “virtual disks”, etc., on Horizon Air infrastructure, to include those leveraged by Horizon Air. 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** – VMware has the necessary policies and procedures to ensure compliance to HIPAA, as well as Information Security best practice, for the Horizon Air platforms. This includes Access Control, Change Control, and Incident Response, as well as many others you would expect to see and need to have in place to ensure both Horizon platforms are controlled environments.

- **Physical safeguards** – The necessary infrastructure, policies, logs, records, and procedures to control physical access to PHI, as well as all customer data, is in place and ensure secure disposal at end of life for all our customers.

- **Technical safeguards** – Horizon Air environments have the right technical safeguards that not only ensure our compliance to regulations such as HIPAA, but also best practice. VMware does not only react to potential risks once identified, we have the technology in place to proactively monitor and alert our operations team should anything or anyone try to gain unauthorized access to our products.

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

But VMware cannot control the way the information is represented, stored, or protected by Horizon Air customers, 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, encryption, etc.).

• **Client and public networks** over which information travels to, from, or within a tenant’s Horizon Air subscription.

• **Policies** by which its clients information from being read by third parties (encryption), grant access to PHI or other data (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.

---

![Diagram](image.png)

**Figure 1.** The “Responsibility Stack”, illustrates the limits of control and areas of individual responsibility for VMware and tenants of its Horizon Air
Joint Responsibilities

Not every HIPAA/HITECH requirement is the exclusive responsibility of one party or another. VMware 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 Horizon Air; tenants manage user accounts to keep authorizations up to date, delete accounts when users leave the organization, etc. Horizon Air customers manage access control to their environment and choose what data is encrypted and to what degree.

• **Firewall** – VMware logically segregates the virtual systems of Horizon 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 Horizon Air 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. This is very important for Horizon Air customers to realize, as they have sole responsibility to ensure their data is backed up and retrievable in the case of disaster.

Overall, organizations complying with HIPAA and HITECH rules are responsible to adopt and use VMware Horizon Air in a manner that achieves and maintains that compliance. Horizon Air is compliant to HIPAA, but many requirements of HIPAA must be addressed specifically by Horizon Air customers.

**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 Horizon 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.