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: