ACHIEVING HIPAA COMPLIANCE WITH RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 introduced a sweeping set of regulations that have had a broad-reaching impact across all areas of the health care industry. Achieving compliance with these regulations, while at the same time minimizing any disruptions to normal business operations, has become a careful balancing act for many enterprise organizations in the health care sector. This paper will illustrate how Red Hat Enterprise Virtualization for Desktops can help these organizations comply with specific HIPAA mandates, while at the same time increasing their overall efficiency and agility.

OVERVIEW OF REGULATIONS

A key objective of HIPAA is to guarantee the privacy of patient information. More specifically, HIPAA seeks the protection of all individually identifiable health information. This includes any information related to an individual's physical or mental health—either past, present, or future. It also includes information regarding any health care or treatment that has been provided to an individual, as well as any financial payments related to that treatment. This information can be further classified as follows:

- **Protected health information (PHI)** – Individually identifiable health information in any form (electronic, written, or oral)
- **Electronic protected health information (EPHI)** – Individually identifiable health information specifically in electronic form

HIPAA seeks the protection of PHI and EPHI by imposing regulations across various individuals and organizations in the health care sector. The law refers to these individuals and organizations as "covered entities," and they include the following:

- Health care providers
- Individual doctors, psychologists, dentists, and chiropractors, as well as facilities such as clinics, nursing homes, and pharmacies.
- Health plans
- Health insurance companies and HMOs, as well as company health plans and government-run programs that pay for health care, such as Medicare, Medicaid, and military and veterans health care programs.
- Health care clearinghouses
- Third-party organizations that process EPHI.
- Medicare prescription drug card sponsors
- Private companies that provide discount drug programs in accordance with the Medicare Modernization Act.

The two most significant provisions of HIPAA are the Privacy Rule and the Security Rule. The Privacy Rule is essentially a patient bill of rights that governs who has access to PHI. It sets standards for how this information can be used and disclosed, while at the same time aiming to ensure that none of its protections stand in the way of high quality care or the health and well-being of the general public.

The Security Rule, on the other hand, deals specifically with EPHI. It defines a set of standards whose objective is to ensure that only those individuals or entities that should be able to access EPHI are actually able to do so. The Security Rule consists of three distinct sets of safeguards:

- **Administrative safeguards** – Address risk assessment, employee clearance and training, access management, and incident handling.
- **Physical safeguards** – Address physical access controls, the security of computers and portable media, and the disposal of EPHI.
- **Technical safeguards** – Address digital access controls, authentication, encryption, and auditing of access.

Some, but not all, of these safeguards have associated implementation specifications. These implementation specifications can be either "required" or "addressable." Required implementation specifications are just that – covered entities are required to implement policies and/or procedures in accordance with the specifications. Addressable implementation specifications, on the other hand, require only that covered entities assess and determine whether or not the specification is reasonable and appropriate for their given environment. If an addressable specification is not implemented, the reason for the non-implementation must be documented and an equivalent alternative measure must be implemented.

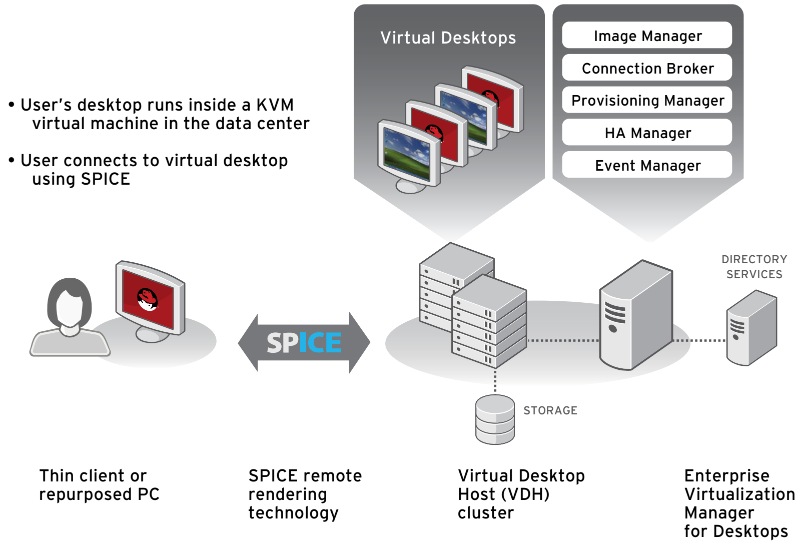
The physical safeguards, in particular, present a unique set of challenges to covered entities having broad deployments of laptops, desktops, and portable media that are used by employees to access or transport EPHI. These devices spend a significant amount of time outside of the organizations' physical boundaries, often in the homes of either employees or patients. Additionally, computers are frequently moved from one location to another within clinical environments. This is particularly the case for devices such as Wireless on Wheels (WOW) mobile workstations, which are explicitly designed for this purpose. This mobility makes it extremely difficult to ensure the security of these devices or to maintain an accurate inventory of the EPHI that resides on them.

In order to more easily comply with the requirements and recommendations of the physical safeguards, a new deployment model is needed for the laptops and desktops used by covered entities. This new deployment model needs to be one in which EPHI is easily protected, inventoried and disposed of, while at the same time being readily accessible by authorized parties.

RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS

The traditional model used by covered entities to deploy desktop computing involves the use of personal computers (PCs). Each of those PCs has a fully-featured operating system installed on it, usually either Windows or Linux, that provides all of the basic computing operations and functions. Applications such as word processors, spreadsheet programs, and web browsers are then installed on top of that operating system in order to provider users with the tools that they need in order to perform their jobs. All of the data associated with the operating system and the applications is stored on the internal hard drive of the PC itself.

RED HAT ENTERPRISE VIRTUALIZATION FOR DESKTOPS


• User's desktop runs inside a KVM virtual machine in the data center
• User connects to virtual desktop using SPICE
Virtual Desktops
Image Manager
Connection Broker
Provisioning Manager
HA Manager
Event Manager
SPICE
DIRECTORY SERVICES
STORAGE
Thin client or repurposed PC
SPICE remote rendering technology
Virtual Desktop Host (VDH) cluster
Enterprise Virtualization Manager for Desktops

With Red Hat Enterprise Virtualization for Desktops, the operating system and applications that make up a user's desktop environment actually reside on servers located in a centralized data center. Users connect to these desktop environments, known as virtual desktops, using a thin client with a network connection and a minimal amount of software installed upon it. Unlike with traditional desktop deployments, no data is stored on these thin clients. This type of architecture is referred to as hosted desktop virtualization.

Red Hat Enterprise Virtualization for Desktops is an end-to-end desktop virtualization solution featuring everything an enterprise needs to deploy virtualized desktops:

- **Red Hat Enterprise Virtualization Hypervisor:** A standalone, high-performance, secure hypervisor based on the Red Hat Enterprise Linux kernel with Kernel-based Virtual Machine (KVM) technology.
- **Red Hat Enterprise Virtualization Manager for Desktops:** a centralized management console with a comprehensive set of management tools that administrators can use to create, monitor, and maintain their virtual desktops.
- **SPICE (Simple Protocol for Independent Computing Environments):** An adaptive remote rendering protocol able to deliver an end user experience comparable to that of a physical desktop.
- **Integrated connection broker:** A web-based portal from which end users can log into their virtual desktops.

By moving desktop environments off of the end point and into the datacenter, Red Hat Enterprise Virtualization for Desktops helps covered entities more easily address the implementation specifications set forth in the physical safeguards. Specifically, many of the specifications of section 164.310(d) (“Device and Media Controls”) are either addressed or made irrelevant with this new architecture:

164.310(d)(2)(i) – Disposal

This required implementation specification mandates that covered entities “implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.” With Red Hat Enterprise Virtualization for Desktops, this specification is much more easily addressed, since no data is ever stored on laptops, desktops, or portable media. The EPHI footprint of the covered entity is essentially reduced to that of the servers in the datacenter on which the virtual desktops are hosted. Disposal policies and procedures therefore only need to be implemented for a small number of servers, as opposed to a vast number of deployed end points and portable media devices.

164.310(d)(2)(ii) – Media Re-use

This required implementation specification mandates that covered entities “implement procedures for removal of electronic protected health information from electronic media before the media are made available.” Much like with specification 164.310(d)(2)(i), the reduced EPHI footprint afforded by Red Hat Enterprise Virtualization for Desktops allows covered entities to easily address this specification. In addition to the reduced data footprint, servers tend to re-purposed much-less frequently than laptops, desktops, or portable media. This reduced frequency further simplifies compliance with this specification for those covered entities deploying Red Hat Enterprise Virtualization for Desktops.

164.310(d)(2)(iii) – Accountability

This addressable implementation specification recommends that covered entities “maintain a record of the movements of hardware and electronic media and any person responsible therefore.” With Red Hat Enterprise Virtualization for Desktops, the laptops and desktops deployed by covered entities can be mobile, but the EPHI for which they're responsible is not. Regardless of where those devices are deployed, the covered entity knows exactly where the EPHI resides at all times—in the safety and security of its datacenters.

164.310(d)(2)(iv) – Data Backup and Storage

This addressable implementation specification recommends that covered entities “create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.” With Red Hat Enterprise Virtualization for Desktops, only the servers on which the virtual desktops are hosted need to be backed up, because it is only there that EPHI resides. This is done is easily and centrally within the datacenter.

In addition to helping covered entities address the implementation specifications set forth in the physical safeguards, Red Hat Enterprise Virtualization for Desktops is designed in such a way that it does not introduce anything that would violate compliance with the standards set forth in the technical safeguards:

164.312(a)(2)(i) – Unique User Identification

This required implementation specification mandates that covered entities “assign a unique name and/or number for identifying and tracking user identity.” Red Hat Enterprise Virtualization for Desktops integrates directly with Active Directory, leveraging the unique user identities and policies that many covered entities already have in place.

164.312(e)(2)(ii) – Encryption

This addressable implementation specification deals with the transmission of EPHI and recommends that covered entities “implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.” Red Hat Enterprise Virtualization for Desktops uses Secure Sockets Layer (SSL) technology to encrypt all communication between virtual desktops and the end point devices used to communicate with them.

BEYOND COMPLIANCE

In addition to helping covered entities achieve HIPAA compliance, Red Hat Enterprise Virtualization for Desktops offers the following benefits:

Increased manageability

With Red Hat Enterprise Virtualization for Desktops, desktop environments can be centrally created, monitored and managed, reducing or even eliminating the need for on-site support in remote clinics or offices.

Increased business agility and continuity

By eliminating the dependencies between the operating system and the underlying hardware, Red Hat Enterprise Virtualization for Desktops allows covered entities to defer desktop replacements and their associated costs. Additionally, this separation allows different operating systems to be accessed from the same device. This is particularly valuable in the case of workstations shared by multiple physicians, nurses, and technicians.

A TRUSTED PARTNER

With a history of over 15 years of providing enterprises with the most secure operating system in the world, there is no better choice than Red Hat for covered entities looking to achieve HIPAA compliance using hosted desktop virtualization. Additionally, Red Hat Enterprise Virtualization for Desktops offers several other unique capabilities and characteristics:

Density

Industry-leading algorithms for memory management allow covered entities to maximize the number of virtual desktops that can be hosted on a single host.

Cross-platform guest support

Support for virtual instances of Red Hat Enterprise Linux Desktop allows covered entities to virtualize both Windows and non-Windows desktops.

Established partner ecosystem

An inherited legacy of over 1,000 certified hardware systems ensures compatibility with current and future systems.

Part of a comprehensive virtualization platform for both desktops and servers

A common infrastructure allows covered entities to manage their complete virtual environments – both desktops and servers.

Open source

No other vendor is as well positioned and suited to bring the power and value of open source to virtualization infrastructures. KVM is open source today, and other components will be made open source in the future.

CONCLUSION

The safeguards outlined in the Health Insurance Portability and Accountability Act (HIPAA) require that individuals and organizations working within the health care sector take decisive action to safeguard patient information. Red Hat Enterprise Virtualization for Desktops represents a new desktop deployment model that significantly simplifies the task of complying with the physical safeguards set forth in HIPAA. By reducing their EPHI footprint and centralizing all data in their data centers, covered entities are able to achieve this compliance while at the same time increasing the manageability and agility of their laptop and desktop deployments.

RED HAT SALES AND INQUIRIES

NORTH AMERICA
1-888-REDHAT1
www.redhat.com

EUROPE, MIDDLE EAST AND AFRICA
00800 7334 2835
www.europe.redhat.com
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

LATIN AMERICA
+54 11 4341 6200
www.latam.redhat.com
info-latam@redhat.com