Business White Paper

The 7 Essential Layers of Secure Cloud Computing

Safeguard your PHI by taking a "Defend the Castle" approach to cloud computing

ClearDATA
SECURE • HEALTHCARE • CLOUD

The 7 Essential Layers of Secure Cloud Computing

Table of Contents

Safeguard Your PHI by Taking a "Defend The Castle" Approach to Cloud Computing

From ancient eras to the modern battlefield, one of the most time-honored military strategies is the concept of "defense in depth," which takes a multi-layered approach to repelling a determined enemy. The core premise is that given sufficient time and resources for an attack, at some point there will be a breach in the protection. But a layered approach – think of a castle with a moat, towers, outer walls, inner walls and a series of inner chambers – gives the defenders time to identify the breach, delay the attackers, and ultimately repel the attack in order to keep the most valuable assets safe.

This sort of layered approach has now become necessary for hospitals and health systems due to the high value cyber criminals place on patient protected health information (PHI). PHI, including names, birth dates, social security numbers, policy numbers and billing information is 10 times more valuable to cyber criminals than credit numbers, according to cybercrime experts. It can be used to open multiple credit lines, create fake IDs, purchase medical equipment or pharmaceuticals that can be resold at a profit and defraud insurance companies, among other issues. And unlike credit card fraud, which usually shows up within days and shut down quickly, stolen PHI can go undetected for months.

Stolen PHI is Growing

Cyber theft of PHI increased 40 percent between 2009 and 2013, according to an annual survey on data detection policy by the Ponemon Institute. The FBI has even gotten involved, alerting medical organizations that hackers had been observed attempting to access healthcare systems with the intention of stealing PHI.

Why the sudden upsurge? It's simple: many healthcare organizations are easy targets. They often lag behind retail and financial organizations in creating hardened, multi-layered approaches to security. In fact, many healthcare organizations are behind in upgrading security systems. With budgets tighter than ever as the healthcare industry transforms from a fee-for-service to pay-for-performance orientation, money is limited. If the decision comes down to upgrading a firewall or purchasing a new MRI machine, the MRI machine wins nearly every time.

The issue is further exacerbated by the many projects to which healthcare IT departments are already committed, such as implementing, upgrading and maintaining their electronic health records (EHR) system, meeting meaningful use objectives and making the conversion from ICD-9 to ICD-10 codes. A lack of budget coupled with a lack of internal resources makes it extremely difficult to keep up with the cyber criminals – especially when the criminals are focused 24/7 on breaching the walls.

The 7 Layers of Defense in Depth

Creating a proper defense in depth requires hardening security at seven distinct layers:

1. **Physical** – data storage in top tier data centers, 24/7 perimeter sensor-monitoring and badged or biometric entry into secure areas. This is an area that is often under-protected within hospitals and health systems.
2. **Network** – enterprise-grade hardware, advanced firewall configuration, SSL VPN security, intrusion detection and prevention, and threat management response. This layer is generally present, but often out-of-date in one or more areas if managed internally.
3. **Application** – data encryption (at rest and in transit), anti-virus protection, patching, two-factor authentication, malware protection and log management. This layer can easily fall behind if patches and upgrades are frequent and internal resources have more pressing tasks.

4 **Server** – file integrity monitoring, patching, role-based access controls and SIEM. Another area that can fall behind without dedicated internal resources.

5 **Data** – backup, at-rest and in-transit encryption, retention, destruction, archiving, SIEM and lifecycle management. This layer often is the primary focus of internal security efforts even though security at all layers is important.

6 **Devices** – mobile and medical devices, as well as BYOD concerns. Often the Achilles heel for internal security because many devices are outside IT's control.

7 **User** – two-factor authentication, social engineering and hacking, policies related to passwords and BYOD, corporate policy, continuous education and ethical hacking. This layer is the most difficult to manage because it requires changing behaviors rather than simply upgrading technology.

These seven layers, which we will examine in this white paper, encompass the three elements the National Security Agency says are core to a complete security strategy: people, technology and operations.

It's rare that a healthcare organization can build this layered defense internally – and then maintain it as cyber criminals shift their method of attack on a daily basis. Fortunately, there is another option.

Not if, but when

It's really not a question of whether a healthcare organization will be targeted by cybercriminals, or if those criminals will be successful in exploiting a weakness in the security. It's a question of when and how much damage will be done – clinically, financially and to the organization's reputation.

Let's take a more in-depth look at the importance of each security layer, how it fits into the overall defense in depth strategy, and how working with a HIPAA-compliant, cloud-based solution provider can help ensure your castle is properly defended against today's threats – and tomorrow's.

Physical Security for Data Centers

What keeps you up at night when it comes to cloud security? Hackers stealing patient data? A server breach that rivals the Target, Home Depot and Adobe incidents? A loss of information?

Those are common concerns. But have you ever thought about the security at the building that physically houses your servers?

Unfortunately, many organizations focus almost exclusively on virtual security – and often nearly forget about the building or room that houses their data, and whether it is properly secured. To be fully secure, a data center has to take into account not only network, data and user security, but physical security as well.

If the physical security of a center is compromised, it could render an entire system unavailable – a scenario that could cause damage to any organization, but is particularly serious to a healthcare provider that relies on systems not only for business management, but for delivering lifesaving patient care.

Landscape and types of physical threats

Visualize the physical infrastructure of a data center. Most centers have similar components: computer servers, telecommunications systems, storage systems, fiber optic cables, power systems and climate control.

Some physical threats are related to malicious intent, like when a thief breaks into a center to steal equipment. Accidental threats can be just as damaging. For instance, what if a system overheats? What if a major storm interrupts power? What if an employee forgets to lock the door at the end of his shift?

These scenarios aren't meant to simply be added to the long list of things you worry about at 3 a.m. In fact, choosing the right data center means you'll never have to think about them again. So how do you find the right data center? Easy, just ask what tier the center is certified as through the Uptime Institute, a third-party research, education and certification consortium for the data center world.

There are four certification levels:

- Tier IV: Fault-tolerant site infrastructure
- Tier III: Concurrently maintainable site infrastructure
- Tier II: Redundant capacity components site infrastructure (redundant)
- Tier I: Basic site infrastructure (non-redundant)

Physical security practices at top tier data centers

Tiers IV and III are considered top-tier data centers. Tier IV is generally reserved for the U.S. government's highest level (top-secret) security data. Tier III data centers meet stringent HIPAA requirements. Tier II, Tier I and uncertified centers are not HIPAA-compliant.

Here are just some examples of what top-tier data centers typically have in place to ensure physical security:

Building Features

- **Safe locations:** Centers are purposely built in safe locations with few natural hazards, like severe weather or seismic issues. It's no accident that many data centers are built in Arizona, a state known for having the least number of natural disasters.
- **Multiple feeds from power substations:** Power is the lifeblood of any data center facility. By balancing the power load across two or more feeds, the operator has the flexibility to adjust in case of power surges, brown outs or complete failure of a single source. It also allows for instant redundancy as there is a lower percentage of power to transfer if a source completely fails.
- **Multiple and disparate conduits for power and bandwidth:** If one conduit is severed, either due to an accident or to vandalism, having multiple feeds into the building for power and Internet is crucial to system availability.
- **Single use, single design:** There's something to be said for buildings designed specifically for secure data storage. They likely have reinforced physical structures such as

concrete bollards, steel-lined walls, bulletproof glass and perimeter fencing.

- **Non multi-tenant:** Threats increase as the number of individuals with access to a building increases. Therefore, a data center should not be located in a multi-tenant facility.

Building security

- **24/7 monitoring:** Physical access is controlled around the clock. On-site technical personnel are also typically available 24/7.
- **Perimeter security:** Video- and/or electronic-surveillance devices are used and security guards are often employed.
- **Two-factor authentication:** To enter, personnel must pass through electronic and identity authentication systems, such as badge and biometric systems.
- **Biometric access:** Involves establishing someone's identity based on chemical, behavioral or physical attributes of that individual.
- **Man traps:** A small room designed to "trap" individuals trying to enter the facility.
- **Backup power security:** Emergency or backup power is used to keep critical data center security equipment operational at all times.
- **Discreet room access and cage or cabinet access:** Access to room is limited; cabinets and cages that house hardware are locked and secure.
- **HVAC systems:** In tier IV centers, the heating, ventilating and air-conditioning (HVAC) systems are not drawing air from outdoors, but are set to recirculate. If there ever were a biological or chemical attack, or heavy smoke, this will protect data center staff and components.

Personnel

- **Authorized personnel-only access:** Only a few employees are allowed to access the data center. Security-escorted entry is recorded by time-stamped logs.

- **Background checks:** Employees are required to pass stringent background checks as well as drug testing. They also must sign confidentiality agreements.
- **Restricted vendor access:** Vendors must carry a photo ID badge and be accompanied by authorized data center personnel at all times.

Reducing or preventing physical threats, along with virtual threats, is key to data security for healthcare organizations. When choosing a data partner, be sure to ask about physical security in addition to virtual security. It'll help your organization to operate at peak effectiveness – and it'll help you sleep better at night.

Network Security

Challenges and requirements on the first line of defense

"Network security" is the first line of defense. Network security refers to physical and software preventive measures an organization takes to protect its network from unauthorized access, misuse, malfunction, modification, destruction and improper disclosure.

When it comes to network security, there is no one-size-fits all solution for healthcare, since each organization is unique, and has unique network vulnerabilities. Therefore, in order to be secure, organizations must build in multiple layers of protection – and be vigilant about maintaining them.

What makes it especially challenging is that building network security is not a project that can be completed and then dropped into maintenance mode. New threats and weaknesses are continually being uncovered, meaning IT must be proactive, continually staying one step ahead of threats. To be successful in maintaining network security, healthcare organizations must invest in the research, people, infrastructure or managed services to drive continual improvement.

Network security threats on the rise

Threats to network security are on the rise for several reasons:

- Hacking used to be about personal glory. Today it's about money. According to a July 2013 study by the Center for Strategic and International Studies and computer security firm McAfee, cybercrime costs U.S. businesses $100 billion each year.
- Healthcare IT resources are more stretched than ever. Technology in the clinical setting has exploded but IT staffing hasn't increased to meet the demands, meaning it is increasingly difficult for them to dedicate resources toward security.
- With large quantities of healthcare applications moving into the mobile sector, securing future platforms is oftentimes put on the back burner due to competing IT priorities and budgetary constraints.

Types of network threats to healthcare

Numerous network security issues threaten healthcare organizations, including:

- Viruses, Trojan horses and "worms" using known signatures
- Attacks by hackers with a specific target in mind
- Spyware or adware driving unmonitored processes (some are relatively harmless, but others are used to steal passwords and gain unauthorized access to the network)
- "Denial of service" attacks designed to interrupt the ability to access information
- Data interception and monetary or identity theft as a result of finding a hole in network security
- Advanced persistent threats that sit silently in the background learning about network weaknesses that can be exploited later
- New viruses for which there is no known signature (called "zero-day" or "zero-hour" attacks) put networks at risk until a patch or defense is developed

An effective network security strategy builds contingencies for all of these threats.

Up until a few years ago, the primary focus for network security was putting technologies in place to prevent the network from being breached. While prevention is still important, the reality is cybercriminals have too much to gain and too many resources to devote for prevention to be a healthcare organization's only strategy. In today's world, detection and rapid remediation are equally critical.

Network security best practices

A layered series of network safeguards and protections include but are not limited to:

Advanced firewall configurations: Robust filters are configured based on the organization's security needs, stopping known threats from attacking the network while allowing legitimate traffic to pass through. They must be constantly maintained and updated with the latest security vulnerability patches or firmware upgrades.

Enterprise-grade hardware: This hardware is designed and certified for enterprise use, and includes the latest security features to reduce vulnerability. Smaller hospitals may be tempted to try to get by with less expensive network hardware (such as consumer routers) that don't incorporate the same level of security, but that's never a good idea. They do not have required feature sets such as web application filtering or intrusion detection system capability.

Intrusion detection and prevention systems (IDPS): These appliances monitor network activities and alert the organization to suspicious activity, allowing time to shut down areas under attack before security can be penetrated.

Network design: The way the network is designed can have a significant impact on preventing, detecting and repelling attacks. Obviously, it should avoid any known security vulnerabilities, adhering to well-established best practices. In healthcare, that includes requirements for HIPAA compliance. It should also incorporate means of isolating detected threats to prevent damage

to the organization while maintaining its ability to function normally. Detection should always include network monitoring to alert the organization when there is a security threat stemming from a vulnerability, access control or other means.

Log management: This invaluable tool detects and traces failed login attempts from known and unknown actors, registry changes, services installed and uninstalled, web server attacks and other suspicious behavior throughout a network. It can trigger advanced firewall changes to lock out unwanted attempts from IP addresses.

Penetration testing: IT should launch periodic planned attacks on its own network (or hire a "white hat" hacking firm) in order to test its defenses and discover security gaps. It is better to discover these security holes internally rather than reacting to them as the result of an actual intruder. There are many organizations that specialize in penetration testing and provide remediation services to help reduce the risk to the organization.

Security information and event management (SIEM): Including appliances, software and managed services, SIEM analyzes security alerts provided by network hardware and applications in real time. It also logs security data and can produce compliance reports. SIEM is particularly helpful in allowing healthcare organizations to correlate data coming in from multiple security sources and recognize unusual activities that don't tie in to a known threat.

Secure Sockets Layer virtual private network (SSL VPN): It functions like traditional VPN, but includes additional connectivity and compatibility, utilizing advanced encryption technology to protect sensitive information. It allows data transmission through an encrypted tunnel to a VPN concentrator, giving the appearance that a user is on a local network, regardless of where he or she is actually located while adding a layer of security for data in transit. Many SSL VPN appliances are also capable of integrating two-factor authentication technologies to enable another layer of security.

Threat management response: Signature-based detection combined with anomaly detection allows security teams to react quickly to known threats, isolating infected computers or devices before the threat becomes pervasive.

Vulnerability testing: This tool proactively identifies vulnerabilities within the IT environment to minimize risk. Vulnerability testing must occur on an ongoing basis in order to remain ahead of cybercriminals that are constantly testing defenses looking for holes to exploit.

Vulnerability monitoring: This involves continuous scanning of the IT infrastructure to identify known weaknesses so they can be remediated quickly. Resources must be dedicated to reviewing incoming data in order to be effective.

Implementing network security best practices ensures your healthcare organization meets mandatory regulatory compliance requirements, such as HIPPA. It also minimizes the risk of litigation from data theft and protects against communication interruption, keeping patients and customers satisfied.

For more information

Read "Considering the Cloud: How Healthcare Organizations Can Keep ePHI Secure."

http://www.cleardata.com/knowledge-hub/considering-the-cloud-how-healthcare-organizations-can-keep-ephi-secure/

Application and Server Security:

Fixing small holes before they become big problems

The past few years have seen tremendous acceleration in the reliance on technology by healthcare organizations. Whether the result of government mandates or healthcare executives recognizing the opportunity to improve clinical quality, drive operational efficiency and lower costs, healthcare organizations are adding new applications in great number.

While that is a good thing, it also adds to an organization's security risks. The more applications there are – both purchased and those developed in-house – the greater the potential for security flaws to be exploited. With network security attacks, there's typically a brute force assault on one area. These attacks are becoming more rare, thanks to technologies such as SSL VPN connectivity and limited public Internet application exposure. But with application security issues (which are on the rise), it's more like an enemy stealthily entering a fortress through small holes in the defenses and then attacking from the inside. The vigilance and resources required to keep up with security patches to protect against known exploits for a multitude of applications is more than most healthcare

organizations can devote. Not to mention the resources it takes to monitor each application to detect and quickly remediate exploits.

In a large healthcare organization, the number of applications and the interactions among them can be highly complex. In fact, each application can potentially interact with dozens of others. In most healthcare settings, there is a tangled web of application interfaces and data, along with a conglomeration of legacy components that have been developed or integrated by multiple divisions within the healthcare organization. For IT, this environment is highly challenging: to find time to simply catalog all their applications, let alone evaluate, prioritize and remediate security issues, is nearly impossible.

Smaller organizations are also at risk. While there may be fewer applications to consider, there are also fewer resources and IT staff to dedicate to security issues. Smaller organizations have less of a buffer to wait while an issue is resolved, so if a critical application goes down, even for a few hours, an organization can be at risk.

In addition to applications, servers are also at risk. Here are examples of security threats to servers:

- Hackers may locate software bugs in the server or its OS and gain access to the server.
- Denial of service (DoS) attacks may be directed to the server.
- Unauthorized parties may read confidential server information.
- Unencrypted or poorly encrypted information being transmitted between the server and the client may be intercepted.
- Hackers can gain access to the network by attacking the server.
- Rogue processes that are not healthcare-specific may be active on the server, causing vulnerabilities that organizations are not aware of.
- Network access ports may be left open by default, allowing for future vulnerabilities.

Understanding application and server security

The term “application security” refers to any methodology designed to ensure that applications adhere to and enforce the

security requirements of the environment in which they are located. It encompasses two considerations. The first is the prevention of unwanted events, such as flaws that may be ingrained in a code that a hacker can exploit. The second is helping ensure desired events occur, such as encryption of confidential patient data. In addition to the obvious preventive measures, such as the implementation of anti-virus and anti-malware software and installing patches as they are made available by the application developers, key best practice elements of application security also include:

Data encryption (at rest and in transit) is the conversion of data into a form that cannot be read without the proper encryption key. While many organizations are diligent about encrypting data in transit by using VPN, secure MPLS or similar technology, encrypting data at rest is an important element of a "defense in depth" strategy. If a cybercriminal is able to break through other defensive layers, encryption at rest provides an extra layer of protection for protected health information and other confidential data.

Two-factor authentication requires a user present not only a username and password but also another form of identification. The second form is generally something the user knows, such as a personal identification number; something the user has, such as an electronic security badge; or something that is inherent to the user, such as a fingerprint or voice print. The latter two in particular are strong defenses against hacking from the outside since they cannot be stolen through key loggers or other electronic means.

Log management detects any failed login attempts from known and unknown actors, any registry changes, any services installed and uninstalled, any web server attacks and other suspicious behavior throughout a network. It is an invaluable tool in detecting not only the occurrence of these actions but also in helping to trace the possible source.

Web application firewalls can significantly improve security, blocking dangerous web application attacks such as SQL injection, cross-site scripting and cross-site request forgeries, an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as

cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked.

Application design also plays an important role in security. Care must be taken when developing applications internally to ensure the methods used follow the best practices for ensuring security. It is especially important when using popular development tools that may introduce a risk through their inclusion. Thorough testing for known application security risks should be incorporated into the overall development plan.

Vulnerability testing involves using tools to proactively identify weaknesses and vulnerabilities within the IT environment so controls can be implemented to minimize those risks. Vulnerability testing must occur on an ongoing basis in order to remain ahead of cybercriminals who are constantly testing defenses looking for holes to exploit.

Code reviews of an internally developed application are necessary in order to locate and repair mistakes overlooked in the initial development phase. This step becomes necessary if a problem or exploit is identified through detection efforts, or the tools that are used to develop the application are discovered to have security flaws. There are many web application code security tools on the market that can scan code for potential vulnerabilities before the code is even merged into production.

Threat management response is signature-based detection combined with anomaly detection to rapidly recognize that something unusual is taking place. It allows security teams to react quickly to known threats, isolating infected computers or devices before the threat becomes pervasive while minimizing false alarms. Many threat management technologies allow for instant notification into a security operations center for immediate escalation and triage.

Servers also rely on FIM and RBAC to stay secure

Servers require oversight in a variety of areas in order to stay secure. Like application security, they rely on patching as well as security information and event management as important

components of the security system. Other best practices for server security:

- File integrity monitoring (FIM): An internal process or control for validating the integrity of the operating system and application software files. As files change, notifications go out to ensure that file changes were intended.
- Role-based access controls (RBAC): An approach that restricts system access to authorized users.

A Cloud-Hosted IT Partner can help ensure application and server security

Clearly, maintaining application and server security requires a great deal of time and effort, as well as properly trained and certified staff. Yet with healthcare IT departments already stretched thin by the projects that are core to the delivery of quality care, as well as the challenges adjusting internal systems to changing reimbursement models, it is often difficult for them to devote the budget and resources required to deliver this level of security.

Working with a HIPAA-compliant cloud provider can relieve this burden while ensuring applications and servers are fully secured. The cloud provider becomes responsible for the security of all applications and servers on their systems, including applying patches as they are issued rather than waiting until they come up in the work queue. In addition, because the applications reside with the cloud provider rather than on individual users' desktops, the entire enterprise can be secured at once rather than waiting until individual computers can be accessed.

Simplifying the Complex

With the proliferation of applications and servers in healthcare and the industry's ever-increasing reliance on technology, ensuring a high level of security is a critical component of a "defense in depth" strategy. With application- and server-based attacks still on the rise, organizations must either dedicate the time, budget and resources to fixing security risks – or work with a cloud provider that can manage it for them.

Data Security

The last line of defense

The core concept behind a "defense in depth" strategy is that any security, no matter how sophisticated or well-maintained, can be breached given sufficient time, resources and determination. Since it is not a question of "if" but "when," having multiple layers of

security delays those who wish to do harm until the threats can be identified and remediated.

Security at the data level provides the last line of defense against cybercriminals, hostile governments and those intent on stealing protected health information (PHI). It is like having a sophisticated safe built into the innermost sanctum of a castle. Even if an enemy scales the outer walls, battles through the inner walls and fights their way into the sanctum itself, they still must open the safe before they can take the crown jewels – i.e. your data.

And don't think that PHI isn't valuable. According to cybercrime experts, PHI is 10 times more valuable than credit card numbers. Stolen PHI can be used to generate far greater illicit revenue, and often goes undetected for months as opposed to credit cards, which are usually shut down within a few hours or days of the data being stolen. Couple that with the fact that healthcare IT departments are inundated with many pressing clinical technology projects (such as EHR implementations and conversion to ICD-10), as well as a shortage of personnel and budgets, and it's easy to see why healthcare is becoming the new favorite target of cybercriminals.

Elements of strong data security

One of the most important security best practices a healthcare organization can follow is to ensure its **data is encrypted at rest as well as in transit**. Data can be intercepted relatively easily when being shared between providers, from a provider to an insurance company, etc.. Encryption methods for data in transit may include technologies that help organizations avoid having to control their data over the public Internet, such as secure MPLS connectivity or SSL VPN-only access to the application. Strong encryption makes the data useless to anyone without the encryption key.

Many organizations believe data is safe while at rest inside their walls. But the moment those walls are penetrated, the PHI is out in the open. Encrypting the data at rest adds a greater degree of difficulty to using the data, and may encourage cybercriminals to seek an easier target whose PHI is not encrypted.

Other measures that are part of a strong data security plan include:

Policies for data retention, archiving and destruction. Any PHI or other confidential data that is legally required to be retained or archived must be stored in compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations, and should be encrypted. This includes archived email, which often contains PHI and other confidential information. Electronic PHI designated for destruction must be removed according to HIPAA requirements, which include using software or hardware products to overwrite media with non-sensitive data (clearing), degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains (purging) or destroying the media containing the PHI completely.

Data lifecycle management. These policies relate to where and how data is stored. Data that is accessed frequently is stored on faster media, while data that is rarely used (such as older X-rays or lab results) can be stored on slower (and less expensive) systems. It is important to ensure that PHI is fully encrypted regardless of where it is in the lifecycle. There are many available technologies that can automatically migrate data from one tier to another based on defined life cycle policies.

Data inventory and safeguards. Managing data properly requires more than HIPAA compliance, as HIPAA only covers PHI. Other types of data must be protected as well. To accomplish that, data must be inventoried so the organization understands all the types of data it has, where it is stored, which systems are accessing it and how it is being used. Appropriate safeguards can then be created that are specific to each data type, such as providing access to financial or human resources data on a "need to know" basis. Some of the technologies used to protect this data may include firewalls, log management, threat management, file integrity monitoring and vulnerability scans.

The alternative: HIPAA-Compliant Cloud Provider

It is obvious that maintaining strong data security internally is a tall, time-consuming order. Fortunately, healthcare organizations can

choose to have their data managed by a HIPAA-compliant cloud provider.

While many organizations may be reluctant to allow PHI to leave their premises due to control concerns, a cloud provider that is focused exclusively on healthcare offers many advantages over on-premises data storage. One of the most important is that data management in all its forms is the cloud provider's primary business, not one part of a larger business as it is for the healthcare organization. As such, the cloud provider makes an extensive investment in ensuring it has all the hardware, software and resources required to deliver the highest level of data security, and that those resources receive constant training in the latest strategies, requirements and technologies for keeping PHI secure.

The cloud provider will also ensure that all PHI is encrypted in-transit and at rest, and will constantly test its systems to ensure that every layer of its defense-in-depth strategy performs to the highest industry standards.

Finally, the cloud provider will monitor the availability, capacity and security of the data through a network operations center. This allows healthcare IT leaders to rest easier knowing their data is secure and their operating costs are reduced from a headcount perspective.

The final line

When personnel and budgets are limited, and multiple high-urgency projects are competing for IT's attention, it's easy for healthcare organizations to fall into the trap of relying on other security measures to protect PHI. Yet those are the circumstances under which PHI becomes most vulnerable.

As the last line of defense, healthcare organizations need to make data security a high priority – or work with a cloud provider that already has the mechanisms and policies in place. There is simply too much at risk to rely on any other course of action.

Mobile and Medical Devices

Cloud-based VDI enhances security in a BYOD environment

The use of mobile technology in healthcare organizations has provided a significant boost for clinician acceptance of information technology. More facilities see the trend toward "bring your own device," or BYOD, as a force for improving care delivery. BYOD programs enable clinicians to use their own personal devices, such as smartphones, notebooks or tablets, to access a hospital's clinical information systems, either within a hospital's walls or offsite.

However, a BYOD approach also involves security risks. Patient information can be accessed if a clinician's mobile device is lost or stolen. Many healthcare organizations have been cited for violating HIPAA security rules when a user's device containing patient health information has been lost, and fines for these violations can total millions of dollars.

One of the best ways for a hospital to mitigate BYOD-related security risks is to use a virtual desktop infrastructure (VDI). This approach enables clinicians to use mobile devices or other types of thin clients to access files, data and applications that are hosted on remote servers. VDI is a proven way to quickly and securely deliver applications and provide access to healthcare systems, enhancing a user's experience and cutting costs. Cloud-based VDI has emerged as an attractive alternative to hosted on-premise VDI implementations.

Advantages of Cloud-based VDI

Until recently, most healthcare organizations hosted their own IT infrastructure, including client/desktops. While giving organizations control over their infrastructure, applications and information, this approach is expensive to install, manage and upgrade.

On-premise VDI removes some level of that work by eliminating the need to manage patches, upgrades and security for endpoint devices. In some cases it also extends the life of those assets since users don't need the latest and greatest computing devices to

work in a VDI environment. Yet IT is still responsible for managing the infrastructure itself – including security, which is critical in healthcare.

To save time and cost, many organizations have migrated to a cloud-based VDI – specifically Desktop-as-a-Service (DaaS) – as an attractive alternative to hosted on-premise VDI implementations. By placing VDI in the cloud, a service provider takes on the responsibility for all operational requirements, including management and maintenance of the VDI infrastructure. Thin clients are used to connect end-users to all cloud-based services.

VDI enhances security with BYOD

A cloud-based VDI approach typically is sufficient to mitigate security risks inherent in a BYOD approach. Moving the client/desktop infrastructure to the cloud places all patient information behind a password-protected firewall. Healthcare data, however, must have additional security in order to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Healthcare organizations considering a move to a cloud-based VDI should ensure that the security measures provided by the partner meet HIPAA requirements.

Additional security considerations include:

- **Encryption** – Adding another layer of protection to patient information. Encrypting hospital- managed data while in motion over the network or at rest in the data center protects the information from all unauthorized personnel.
- **Multi-factor authentication** – Rather than require a simple username and password, multi-factor authentication requires the presentation of two or more of the three authentication factors: a knowledge factor (something the user "knows"), a possession factor (something the user "has"), and an inherence factor (something the user "is"). After presentation, each factor must be validated by the other party for authentication.
- **Role-based delivery of information** – Depending on a person's role within the healthcare environment, only certain patient information is accessible.

With such security measures in place, VDI can without question improve security on the user end without IT having to secure each individual device. Consider that protected health information (PHI) that is downloaded to a mobile device is at high risk of exposure. For example, if a mobile device containing patient data is lost or stolen, the information is compromised. Breaches of this type must be reported to federal agencies, and are very costly in terms of reputation and money.

With cloud-based VDI, when clinicians use their own devices – thin clients, notebooks, tablets or smartphones – they click on a desktop icon and instantaneously receive a virtual desktop running in the cloud. PHI is kept safe behind the data center firewall, and organizations are able to more easily meet compliance requirements.

The enablement of BYOD in healthcare is a major force in encouraging clinician use of digitized health information. The use of cloud-based VDI can play a key role in increasing provider productivity and helping to rein in IT department expenses, while mitigating growing risks of HIPAA violations and other regulatory compliance concerns.

Leveraging Cloud-based VDI for medical devices means greater security for patients, providers

Medical devices help improve patient outcomes and can save lives, and dozens of new technologies are approved by the U.S. Food and Drug Administration (FDA) each year.

However, the increasing availability and use of medical devices is also leading to increased security risks. Additionally, not only are more medical devices becoming available, increasingly hackers and others intent on doing damage are developing more ways to access them, often through technology – and they are becoming more determined and sophisticated in their efforts.

What's the incentive? Accessing a medical device gives thieves an array of information and options:

- Access to protected health information (PHI). Some estimate that having PHI is 10 times more valuable than credit card data.

PHI also has a longer shelf life than credit cards, and correcting or purging fraud is more challenging with medical records than with credit cards.

- The ability to cause physical harm to a patient.
- Illegal and bogus treatment by corrupt providers or fake clinics.
- Purchase of drugs for use by addicts or resale.
- Obtaining free treatment by impersonating a health plan member.

Here are examples of some of the most vulnerable devices, and how thieves and others can access them and other related equipment in order to put patients and providers at serious risk:

Drug Infusion Pumps: These medical devices, which are most often used to deliver morphine drips, chemotherapy and antibiotics, can be accessed remotely, then manipulated in order to change the dosage delivered to a patient.

Implantable Cardiac Defibrillators: Many are Bluetooth-enabled, and if that Bluetooth is hacked, someone intent on doing harm can deliver random shocks to a patient's heart, or they can stop a medically needed shock from occurring.

X-Rays: Hackers can access a hospital's network to damage or manipulate x-rays.

CT Scanners: Hackers can alter configuration files and change the amount of radiation patients receive.

Refrigeration Units: Temperature settings can be deliberately reset, in order to cause blood or drugs to spoil

Electronic Medical Records: Can be altered, causing clinicians to misdiagnose, administer improper care or prescribe the wrong medications.

Damage continues, even after a security breach

Plus, if a security breach occurs and PHI is stolen or a patient is harmed, the healthcare organization can suffer near catastrophic

damage, as HIPPA or other federal and state regulators step in to impose fines and lawyers appear to file lawsuits.

How to begin strengthening security around medical devices and PHI

Fortunately, there are steps a hospital or healthcare organization can begin taking today to strengthen their security around medical devices, as well as overall security related to PHI. They include:

- Inventory your medical devices
- Perform a risk analysis – and ensure it is a continued process
- Identify administrative weaknesses
- Document your policies and procedures
- Identify physical threats
- Identify and mitigate technological threats
- Build your circle of trust
- Create corrective action plans

Using VDI is one of the best ways to reduce threats related to medical devices

One of the best ways for a hospital or other healthcare organization to begin to reduce medical device-related security risk is to adopt a virtual desktop infrastructure (VDI). VDI allows clinicians to securely access files, data and applications related to medical devices that are hosted on remote servers. VDI is a proven way to quickly and securely deliver applications and provide access to healthcare systems, enhancing a user's experience and cutting costs. Cloud-based VDI has emerged as an attractive alternative to hosted on-premise VDI implementations as VDI removes the security risk resulting from lost or stolen devices.

Advantages of Cloud-based VDI

Until recently, most healthcare organizations hosted their own IT infrastructure, including client/desktops. While giving organizations control over their infrastructure, applications and information, this approach is expensive to install, manage and upgrade.

On-premise VDI removes some level of that work by eliminating the need to manage patches, upgrades and security for endpoint devices. In some cases it also extends the life of those assets since users don't need the latest and greatest computing devices to work in a VDI environment. Yet IT is still responsible for managing the infrastructure itself – including security, which is critical in healthcare.

To save time and cost, many organizations have migrated to a cloud-based VDI – specifically Desktop-as-a-Service (DaaS) – as an attractive alternative to hosted on-premise VDI implementations. By placing VDI in the cloud, a service provider takes on the responsibility for all operational requirements, including management and maintenance of the VDI infrastructure. Thin clients are used to connect end-users to all cloud-based services.

VDI enhances security with medical devices

A cloud-based VDI approach typically is sufficient to mitigate security risks inherent in medical devices. Moving the client/desktop infrastructure to the cloud places all patient information behind an encrypted and highly available firewall. Healthcare data, however, must have additional security in order to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Healthcare organizations considering a move to a cloud-based VDI should ensure that the security measures provided by the partner meet HIPAA requirements.

With proper security measures in place, VDI can without question improve security on the user end without IT having to secure each individual device. With cloud-based VDI, when clinicians use medical devices – they click on a desktop icon and instantaneously receive a virtual desktop running in the cloud. PHI is kept safe behind the data center firewall, and organizations are able to more easily meet compliance requirements.

The enablement of telehealth through medical devices is a major force in managing costs and improving patient outcomes. The use of cloud-based VDI can play a key role in increasing provider productivity while mitigating growing risks of HIPAA violations and other regulatory compliance concerns.

Users

The weakest link in healthcare data center security

Of all the seven layers of a comprehensive "defense in depth" security strategy for protected health information (PHI) – one which includes multiple, overlapping measures to guard against the breach of any single layer becoming catastrophic – the weakest link by far is the users.

Securing the other six layers primarily relies on applying and maintaining the appropriate technologies. While this can be a costly, time-and-resource-intensive process, it is also very predictable. While there are some elements of policy to be enacted, in general compliance with those policies can be verified and controlled with relative ease.

User security, on the other hand, often revolves around changing or controlling human behavior. This is a far greater challenge for IT.

What makes it so difficult is that healthcare organizations are not trying to keep users out of the system or away from PHI. Users must be allowed access in order to do their jobs. As a result they have automatically bypassed most of the security protocols the organization has put in place; a security plan that focuses solely on technology or intruder prevention leaves PHI extremely vulnerable to problems from the inside. In addition, the number of weak points is equal to the number of users; in a large healthcare organization, keeping tabs on all of them is an almost impossible task – especially with IT already being pressed to do more with less.

The user risks

Risks from users come in several different forms. The most obvious is the disgruntled or nefarious employee who intentionally uses their position to steal information or cause harm. An employee who has been terminated, for example, may steal PHI or financial data, delete files or purposely introduce a virus or worm into the system to seek revenge. Someone intent on stealing PHI may seek a job with computer access within the organization – even a low-level job – as a means of bypassing external-facing security.

Then there are those who inadvertently allow others access to PHI. One widespread technique for cybercriminals to gain access to PHI is through social engineering. Former "black hat" hackers generally agree that getting a user to provide network access through social engineering is far faster and easier than hacking the network from the outside.

A favorite technique of cybercriminals is to send an email that appears to be from a friend of the user asking him or her to click on a link to see a funny video or some other innocuous request. They may also send an email that appears to be from a package delivery service, a bank, the IRS or some other legitimate organization. In these cases the email will describe a problem that will cause the user to worry, and urging them to follow a link to resolve the problem.

When the user clicks on the link software is downloaded onto that computer which opens a window into the network. Sometimes the software is designed to act immediately. Other times, such as with advanced persistent threats (APTs), it sneaks onto the network and sits quietly, learning all it can about the security protocols – sometimes for months. When it finally "phones home" it details opportunities for access that will be difficult to detect because they appear to be normal activity.

Another means of gaining access is through public Wi-Fi connections. A cybercriminal can set up shop in a coffee house or other location frequented by employees of the targeted healthcare organization. When an employee connects to the location's free Wi-Fi to check their email or perform some other action, the cybercriminal can not only steal unencrypted data as it crosses the network, he or she can piggyback on that connection and gain access in a way that looks like normal traffic to network security.

Then, of course, there is the lost or stolen device – especially if it is set up to remember the user's password and give him or her instant access to applications. That is like walking through the front door and being handed the keys to the data center.

Filling the user-sized security holes

Changing human behavior is not easy, nor is it quick. There are no "patches" or downloads that can be implemented into the brains of users to upgrade protection. Instead, it requires a continuous effort and constant vigilance around:

Policies and procedures – IT must establish and enforce formal, documented policies around every aspect of data access.

Included should be policies for:

- Identifying the security executive responsible for developing, implementing, monitoring and communicating HIPAA-compliant security
- Authorization of who is allowed to access and work with PHI
- Permissions for their level of access
- Where access to PHI is and is not allowed
- Devices on which access to different types of data is allowed
- Detection of security incidents
- Sanctions for employees who do not follow policies
- Constant re-education on policies and procedures with refresher courses on user security

IT must also work with other departments, especially Human Resources, so the people responsible for security are aware of changes (such as terminations) that could constitute threats and get ahead of them. Interestingly, one of the most-overlooked areas is the resignation or termination of network administrators or other trusted IT personnel with high-level access. Cases have been documented where former employees maintained access for months after leaving the organization. A former employee, particularly an unhappy one, with deep IT expertise and full access to the organization's PHI and other highly confidential data represents significant danger.

Passwords and user authentication – The use of strong (random letter, number and symbol combination) passwords is much-

debated. While a random series of characters is more difficult to guess, it is also more difficult for users to remember – which leads to them writing the password on a sticky note and attaching it to a monitor or placing it inside a drawer –
either of which can be easily stolen. The best passwords are those that mean something to the user but cannot be easily guessed.

Two-factor authentication provides greater protection of PHI. This method involves not only something the user knows (password), but also something the user has (such as a proximity badge) and something inherent to the user (fingerprint, voice print). With this method, even if the password is stolen or hacked access is still denied or delayed, giving the organization time to react. In the past many healthcare organizations avoided utilizing two-factor due to maintenance, licensing, and training. Today, almost every two-factor authentication technology vendor has mobile and soft token capability, so that maintaining physical key fobs is no longer needed..

BYOD policies – In today's world, users are demanding the ability to use their own devices (smartphones, tablets) to access the applications and data they need to perform their jobs. While it offers many benefits, it also creates great risk to the organization. Specific policies, procedures and requirements – such as the use of passwords and biometric data (where available) to access the device – must be enacted and vigorously enforced to prevent the type of data loss that makes headlines. With technologies such as VNA viewers clinicians no longer need to download PHI onto a BYOD device thus removing this common user security risk.

User training – Once policies and procedures are established, users must be trained on them. Not once, but on a regular basis. The organization should also periodically test user knowledge and adherence to security protocols to close gaps in performance and educate users on the importance of following corporate mandates. This is particularly important for users who take their devices outside the protected environment of the healthcare organization. Devices should be inspected and tested as well to ensure they are in compliance with the organization's policies.

Vulnerability testing – User security policies and procedures should be tested through periodic ethical (white hat) hacking to determine if users are following them. For example, testers can send social engineering-type emails to see who clicks on the links. Any holes should be addressed immediately and included as part of the user education.

A Cloud provider can reduce the workload

Working with a cloud provider can relieve many of the security risks users represent, providing stronger protection of PHI while allowing healthcare organizations to concentrate their resources on areas only they can manage. Even when organizations have deployed diligent policies around user security, there is rarely time to enforce the monitoring around these policies, which is what a cloud provider can bring to the
healthcare organization.

One of the most significant contributions a cloud provider can make is virtualizing applications and data (including PHI). Rather than downloading PHI to a device, the applications and data remain on the cloud provider's servers and are merely "viewed" with the device. In that way, if a device is lost or stolen no PHI remains on it.

A cloud provider will also have security protocols in place to look for unusual activities, such as multiple incorrect attempts to enter a password, or passwords being entered without the second form of authentication when two factor authentication is in place, and monitor them 24/7. The provider will determine the nature of the problem before alerting the healthcare organization's internal security team, helping eliminate the issue of false positives and alarm fatigue. They will also take on the responsibility of vulnerability testing, normally as part of the overall contract.

Finally, a cloud provider that is focused exclusively on healthcare can use their depth of experience across many clients to help the organization develop policies and procedures that are HIPAA-compliant as well as meeting other healthcare security standards, and deliver continuous training and education to the organization's users.

Strengthening the weak link

Whether the cause is intentional or inadvertent, there is little question among security experts that users pose the greatest risk to PHI and other data. They are the weakest link because they provide multiple points of entry, and are the most difficult to control.

Without a strong, concerted effort in this area, healthcare organizations are very vulnerable no matter what other security measures they have in place. A cloud-based provider can be invaluable in strengthening security around users – and then making sure policies and protocols are followed. All while ensuring properly authorized users have access to the applications and data they require.

Making a "Defense In Depth" Strategy Work

For IT professionals, building and maintaining security is an important task for IT, but it is merely one of many. For cybercriminals, however, breaking security is their primary business. And a very lucrative one. As such, they can devote more time and resources to the attack than internal IT departments will ever be able to bring to the defense. Which means a breach is inevitable in the face of a determined attacker.

The risk goes up exponentially for healthcare organizations due to the selling price and long-term value of PHI; the more valuable the target, the more determined the opponent will be. That is why having a fully realized "defense in depth" strategy, where all seven layers of security are hardened to the maximum industry standards, is so critical to avoiding the type of data breaches that make headlines.

As we have seen, each of the seven layers requires very specific and detailed expertise. It is unrealistic to expect internal IT generalists to be sufficiently knowledgeable across all of these areas. To protect their PHI, healthcare organizations today must invest in acquiring the right technology and expertise across all seven layers.

Yet adding hardware, software and internal experts at a time IT is already being asked to do more with less will be a difficult sell at best. At least until something catastrophic occurs.

Moving PHI to a HIPAA-compliant cloud provider with systems developed specifically for the healthcare industry provides a highly reliable yet cost-effective alternative. Because data management is their primary focus, the cloud provider will already have a defense in depth strategy in place, along with the leading-edge security technology, expertise and volume of resources to keep it operating at peak efficiency. They will have certified personnel who spend their entire workdays looking for and repelling possible attacks rather than reacting to them once they are successful. All of which is included automatically as part of the data management contract.

On the rare occasion there is a breach at any one layer, the strength of the others will prevent it from damaging the healthcare organization. And, of course, the more difficult access to PHI becomes, the more likely cybercriminals will be to redirect their efforts toward easier targets. Because the best way to safeguard PHI is to discourage attacks in the first place.

The clock is ticking. And the consequences of failing to take the appropriate actions are substantial. A cloud provider can help ensure your organization becomes secure at all seven layers so it is properly prepared to defend the castle – and the PHI riches within.

To learn more about how a HIPAA-compliant cloud provider can help your organization protect PHI more effectively, call (800) 804-6052 or go to www.cleardata.com

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. More than 310,000 healthcare professionals rely on ClearDATA's HIPAA compliant cloud computing HealthDATA platform and infrastructure to store, manage, protect and share their patient data and critical applications.

For more information

101 W. 6th Street, Ste. 300, Austin, TX 78745

(833) 992-5327

www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD