Business White Paper

Five Common Ways Technology Vendors Put Protected Health Information (PHI) At Risk

ClearDATA
SECURE • HEALTHCARE • CLOUD

Five Common Ways Technology Vendors Put Protected Health Information (PHI) At Risk

Table of Contents

Healthcare IT vendors play a critical role for healthcare systems, helping them to manage enormous amounts of data in order to increase efficiency, improve patient care and improve financial performance. Unfortunately, IT vendors sometimes create new security gaps and with them new opportunities for data breaches to occur. Healthcare PHI breaches resulting from technology vendor mistakes and misunderstandings have increased over the past few years.

ClearDATA sees five common scenarios where technology vendors can inadvertently create a vulnerable environment. They are:

- Failure to assess risk
- Lack of awareness regarding system activity
- Failure to maintain the system with software patches
- Lack of training
- No approach to change management

The breaches that result from such vulnerabilities destroy patient privacy and can irreparably harm an IT vendor's reputation. This white paper will discuss each of these five vulnerabilities in detail in order to help IT vendors understand the threats that exist and how to address them.

1. Failure to Assess Risk

With each new headline of another healthcare data breach, one question becomes ever more urgent for healthcare technology vendors to answer. Are they adequately safeguarding the protected healthcare information under their watch? The reality is many won't know the answer until after a data breach occurs.

Given the rise in such incidents—and the stressful toll they take on patients whose private health information has been obtained by cyber criminals to commit medical fraud or even blackmail—this needs to change. Healthcare technology vendors must commit to closing off every possible avenue of risk of the medical records and other health data in their systems. And that starts with scoping out just how much at risk these systems are.

The HIPAA Security Rule requires that certain organizations, known as covered entities and business associates, regularly perform risk assessments. Yet 33 percent never have, increasing the rate of healthcare data breaches.[1] The public would be troubled to learn this statistic, especially now that one in 10 Americans has been affected by a healthcare data breach.

Action items

Perform annual risk assessments

Many healthcare technology vendors struggle to find enough staff time to conduct risk assessments. It's intensive work, multi-layered and IT professionals must know what to look for. Further, a one-time risk assessment is not enough; at minimum, such assessments should take place annually.

The basic framework of a security risk assessment[2]:

- Conduct a periodic review of data inventories and critical assets
- Assess the administrative, physical and technical safeguards in place to protect healthcare data
- Perform regular re-evaluations of risk (repeat the above two steps)

1. 2014 - State Of Risk Report
Based On A Survey Commissioned By Trustwave

https://www2.trustwave.com/rs/trustwave/images/2014_TW_StateofRiskReport.pdf

2. Security Risk Assessment

https://www.cleardata.com/solutions/hipaa-security-risk-assessment-sra/

The best way to assure such a rigorous security philosophy is followed? Appoint a chief privacy officer—and one who is actually in the game, not just a figure head.

Inventory your PHI

Another important component of a security risk assessment: know where your protected health information is stored. Otherwise, how will you know you have the appropriate safeguards in place? Conduct an inventory so you know where this data is, in which applications[1] and who has access to it. That way, in the event of a breach, you'll be able to quickly report it and shut it down.

While this in itself may be of small comfort, it is nothing less than stunning how long so many breaches go undetected. In fact, research shows that only 5 percent[2] of breaches are discovered within three months of entry. On that note, if the breach exceeds more than 500 records, or you don't know how many records were compromised, you must report it to the Office of Civil Rights (OCR).

Perform annual pen testing

Penetration testing, or pen testing for short, should be done on at least an annual basis by professionals who are hired to ethically hack into your systems. Very often they may find entry via an outdated, unsupported operating system or software. Some examples: Microsoft XP, SQL 2003, to name just a couple. Such systems and apps should be retired as part of a sound risk management policy. In a related suggestion, so should data after a certain period of time. A data lifecycle map is essential here.

Hire a security risk assessment partner

Exceeding, not just meeting HIPAA compliance must be the goal to stay ahead of hackers determined to crack your network. If you have any doubts about your organization's IT security expertise or availability in time to perform a security risk assessment, it is most definitely the wiser course to partner with a specialist in this area.

1. Critical Security Suite

https://www.cleardata.com/solutions/critical-security-suite/

2. 2014 Year Of The Mega Breach PDF

Ponemon Institute© Research Report

http://www.ponemon.org/local/upload/file/2014 The Year of the Mega Breach FINAL_3.pdf

Typical credentials of a partner well-versed in security risk assessments include:

- HITRUST-Certification
- Onsite chief privacy officer (CIPP/US, CIPP/IT Certified)
- Mandatory HIPAA training for all employees

Such a partner will be able to quickly determine just how at risk you—and by extension your customers—are for a data breach. And "quickly" is the operative word here. Taking a "wait and see" approach is a waiting game that, in the end, only the hackers win.

2. Lack of awareness regarding system activity

Unaware, unauthorized and unsafe—that's "Shadow IT" in a nutshell. The proliferation within companies of apps and hardware that bypasses official approval from IT has become so common, some professional analysts suggest just embracing it and servicing whatever technology employees want. Maybe that's an option for companies that aren't responsible by law to safeguard patient records and other protected health information. But for healthcare IT companies that serve providers, payers and others in the healthcare landscape, security will always be the first concern. They are a common access point to patient records—and cyber thieves know it. Healthcare IT vendors simply can't afford to have the kind of unmanaged and unsecured applications and devices that these criminals depend on for a gateway into valuable protected health information.

Most IT departments are working through an unending list of tasks, each considered the "highest priority" by those in need. Many times, employees choose not to wait for IT assistance and instead seek out software, hardware or services on their own, including various web-based services. While they may feel like they're being efficient, the reality is they frequently overlook the security and regulatory requirements of the healthcare environment—including

HIPAA-mandated safeguards for protected health information. Even worse than a stiff fine in the event of a breach, these shadow IT projects expose patients to the stress of what could be a lifelong battle to reclaim their stolen medical identity.

Action items

Take a multi-pronged approach

A multi-pronged approach to the shadow IT problem starts with company-wide education on the serious risks employees are taking both with the company's reputation and the patient data it's tasked with protecting. In parallel to this effort, a comprehensive security risk assessment should take place that accounts for every application, system, device and piece of equipment that could serve as a cybercriminal bridge to protected health information. While taking inventory of all these assets may seem like a daunting project, it can be successfully done with the help of a cloud managed services vendor with extensive experience in the healthcare industry. Indeed, a healthcare-specific vendor will know what to look for and where, and can also perform penetration tests on each asset to determine its risk level.

Outsource configuration management

How can healthcare IT vendors make sure shadow IT won't return? An increasingly high number are deciding to simply migrate their entire IT infrastructure to the cloud. From there, it's a matter of picking and choosing which centralized security services are needed. Configuration management, for example, is a useful service in the realm of change management—that is, whenever an organization brings new devices, apps and systems on board. Configuration management makes sure, among other items, that vendor-supplied credentials are changed to unique passwords. This is of paramount importance; breaches have been traced back to hackers using an app or device's vendor-default credentials (which are readily available on the black market).

Manage log monitoring

Another valuable service is managed log monitoring and management that delivers 24×7 security monitoring of log data and immediately identifies potential security and compliance issues. Paired with managed intrusion prevention and threat-resolution services, it offers the around-the-clock monitoring needed to protect data that is otherwise continuously at risk.

Working with an experienced managed services partner that understands the unique challenges and security risks involved with healthcare IT can remove the problems caused when an organization lacks awareness of what's happening with their IT infrastructure. It's a simple and, more importantly, effective way to transform the stress of system unawareness into confidence and peace of mind that all systems and IT activities are accounted for—and protected.

3. Failure to maintain the system with software patches

While risk assessment and shadow IT are two areas of vulnerability where problems can exist through no fault of the IT vendor, there are others where it is the vendor's (or users') inaction that create the problem. One example is the failure to keep up with software patches.

It's no secret that regularly applying system updates and patches is one of the most important and effective ways to plug security holes and safeguard your data. Yet, stories are told every day about major healthcare system breaches resulting from well-known software or hardware vulnerabilities.

More times than not, it's a failure to develop, implement, and follow a rigorous maintenance plan. It's well known among IT professionals that applying system upgrades can be a hassle. Some may even believe it is more trouble than its worth. It requires

working late nights to avoid disrupting critical systems during peak patient hours. Upgrades can negatively impact the stability of your infrastructure resulting in many hours of troubleshooting and rework.

The alternative is much worse, especially in the healthcare industry.

Action items

Be proactive

In 2014, Anchorage Community Mental Health Services (ACMHS) was assessed a $150,000 fine from the U.S. Dept. of Health and Human Services (HHS) when nearly 3,000 patients had their data accessed illegally via a malware breach because ACMHS failed to patch their systems and continued to run outdated and unsupported software for a seven-year period from 2005 to 2012. In addition to the $150,000 payment, ACMHS will also be required to implement a corrective action plan (CAP) and provide regular reports to the HHS on the progression and status of its compliance program.

Proper planning and documentation is key. Instead of reacting to patches as they come in and relying on software vendors to be responsible for sending notification of patch availability, it is wise to make patching a regular part of the IT schedule and budget. Being proactive reduces the risk that a critical patch or update is missed.

Bring in reinforcements

The solution to safeguarding your systems is a documented plan that details all impacted software and applications and includes a patching plan. It might be wise to start with a risk assessment from a trusted third-party information security services provider. They can quickly ascertain which software and applications require the most effort to maintain and create a comprehensive plan for security updates. They can even take on the work of applying the patches and work with software vendors and developers to understand when they plan to offer routine patches.

Four steps a managed data services provider can help take for a successful patching plan are:

1 Test the Patch

Before any patch goes live, it should be tested to make sure it will work properly within all impacted applications and operating systems. Using the same application or database code in testing allows you to reveal any problems or potential failures before they can negatively affect working systems.

2 Make the patch accessible and simple to implement

Patches should be designed to be implemented in as few steps as possible. Complicated instructions only serve to reinforce the perception among users that these patches are a bother, as opposed to a critical necessity.

3 Monitor the status of the patch

Once the patch is made available it is critical to monitor it for problems. Unexpected bugs or complications can result in additional vulnerabilities. Work isn't done when the patch goes live, monitoring is necessary to make sure it is working toward its intended purpose and that there aren't unforeseen issues keeping it from being successfully downloaded and installed.

4 Monitor user compliance in implementing the patch

Additional monitoring is necessary to make sure that users are indeed downloading the patch. Anything but a high install rate may be an indicator of technical issues, or it may simply point out the need for additional outreach to users. Users may require additional education regarding the critical importance of these patches and the security risks associated with ignoring them.

Bottom line, receiving and acting on patch notifications is a continuous responsibility. You can't count on hackers ever taking a day off. If an emergency patch is made available on Christmas Day, someone must be available to implement it in order to protect the organization—and most importantly, patient data.

4. Lack of training

Regardless of how much money is invested in purchasing and implementing the latest and greatest software and hardware to keep data secure, all of it can be undone by improper and incomplete training. Consider the following scenario:

> A doctor, on her way out of the office for the weekend, realizes that she forgot to check a patient record to make sure that patient was prescribed the correct medication. As an assistant pulls that record, he inadvertently moves the mousepad. The doctor notices that underneath the pad is a piece of paper taped to the desk. On that paper is written the user name and password for the computer system.

This type of scenario is commonplace, despite the fact that mandatory training requirements exist that should prevent it. General Security Awareness training is a HIPAA requirement, and while easy to do in theory, there are other things to consider. Some examples of the topics covered in mandatory HIPAA training include:

- Assignment of a privacy and security officer for your organization
- Developing a procedure for reporting complaints or violations
- Confidentiality policies and procedures
- Security policies and procedures
- Governing laws and regulations
- Patient rights
- Physical and workstation security
- Cyber security best practices; prevention, monitoring, and response
- Social media policies and procedures

Proper training needs to be a priority, but often isn't due to the lack of understanding of its importance. This lack of recognition about the critical nature of training is apparent by how few

training resources exist. Few organizations possess staffers or tools dedicated to in-house security awareness training. Focused on the day-to-day, many organizations view this training as a waste of time and are reluctant to pull people away from their core duties in order to complete it.

Additionally, many organizations don't have the in-house personnel who understand the technical nature of IT in order to develop or guide others through security training. Taken all together, these factors can lead to employee negligence, which according to the Ponemon Institute's Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data (May 2015), is the biggest source for worry concerning security among healthcare organizations.

Action items

Identify gaps in user training

Working with a managed data service provider to complete a full risk assessment is an effective way of recognizing potential gaps in user training. Managed data service experts possess the knowledge of HIPAA compliance as well as experience and access to innovative programs such as the Open Web Application Security Project (OWASP). This global initiative aims to improve the overall security of web-based solutions and is an excellent resource for any third-party software vendor that seeks to help healthcare organizations protect their data.

OWASP's top ten vulnerabilities related to lack of training are:

- Unvalidated parameters
- Broken access control
- Broken account and session management
- Cross-site scripting flaws (XSS)
- Buffer overflows
- Command injection flaws
- Error handling flaws

- Insecure use of cryptography
- Remote administration flaws
- Web and app server misconfiguration

Appoint a training champion

In order to address these vulnerabilities effectively, training must be a priority. Appoint one person as a champion for training; that person should be tasked with keeping up with an organization's vulnerabilities and implementing the proper training to address them. Dedicating one or more people to manage training is important – it eliminates the feeling that others are being pulled away from high value tasks and shows the organization's commitment to training as a critical function. Identify a member of the IT department to be accountable for scheduling and overseeing training, ensuring it takes place. It helps to identify members of the organization who can be recognized as thought leaders in data security, providing a go-to individual for other employees who may have questions. If in-house resources are not available to create, conduct or manage the training program, third-party vendors who are familiar with cloud-based security are a proven resource.

5. Change management

So far, this paper has discussed a number of issues related directly to the data system and how vendors and users interact with it. But vulnerabilities also arrive indirectly through channels that might not be on the radar of the internal customer IT team, much less the IT vendor. One instance where this is true is during organizational change. Every day there is news of one healthcare system acquiring another in order to merge service sets and realize new efficiencies. These periods of change are often chaotic, particularly when it pertains to merging data systems while trying to maintain data security.

Periods of change are when organizations are most vulnerable to security breaches—especially healthcare entities and the technology

vendors that serve them. During these periods, many things are often happening at once:

- New hardware and/or software is added to the greater system's IT network
- New mobile devices and applications are added, often without alerting IT
- Disparate IT protocols are often occurring simultaneously in the period before one uniform practice is decided upon and adopted system-wide
- Different patient databases are combined

The scary truth is that only a little more than half of organizations apply the necessary change management principles[1] to their IT assets. According to a study of configuration management[2] for cloud-based infrastructures, 80 percent of outages impacting mission-critical services will be caused by people and process issues and 50 percent of those outages will be caused by issues related to handing off the system to new personnel.

During this time, the system is ripe for unplanned and/or unapproved alterations. To put this into perspective, the cost of such downtime is approximately $8,000 per minute for the healthcare provider, not to mention the cost to an IT vendor's reputation.

Action items

Create an integration plan

The answer to this problem lies in making sure that managing change contains a plan for the integration of all IT services, particularly those that put valuable patient data at risk. However, many healthcare IT organizations lack the resources to fully address the staffing needs required during organizational change. At these times, it may be smart to enlist the support of an expert managed services company that specializes in healthcare cloud security and management. These vendors possess the expertise necessary to help IT vendors recognize and address system vulnerabilities before they become exploited.

1. 2014 State of Risk Report

The 2014 State of Risk Report from Trustwave shows that many businesses actually are taking on a huge amount of preventable security risk.

https://www2.trustwave.com/2014-State-of-Risk-Report.html

2. Top Seven Considerations for Configuration Management for Virtual and Cloud Infrastructures

Gartner - As IT organizations add various cloud architectures to address changing user needs, it is critical to rightsize configuration management. This research provides seven considerations for rightsizing configuration management processes.

https://www.gartner.com/doc/1458132/overview-top-seven-considerations-configuration

Explore third party resources

There are infrastructure and information security services tailored specifically to the needs of change management. One such service is configuration management, which assures (among other responsibilities) that vendor-supplied credentials are changed to unique passwords. These managed data service experts can also handle security, monitoring, patch management and other professional services. They can also help to manage a secure transition of valuable data to new systems and aid in the integration of multiple databases. After the initial integration, managed services can include real-time monitoring, intrusion detection and prevention, data encryption and regular scans to detect new compliance risks.

Understand best practices

A useful resource is the IT Process Institute's Visible Ops Handbook[1]. This comprehensive guide provides direction to IT vendors on many aspects of managing organizational change and translating that to the IT infrastructure. This includes such security measures as reducing access to systems that can be modified, the importance of documenting all information related to IT assets, how to build a RACI, how to create a repeatable build library and making continuous improvement a part of the daily culture.

However it is accomplished, healthcare IT vendors must learn to recognize periods of change are tried and true opportunities for data breaches. Having plans and policies in place for change management is key to thwarting them.

Conclusion

Despite the profoundly negative impact of patient data breaches, only five percent of organizations affected resolve the underlying security issue within a month. The vast majority are resolved months or more than a year later, or never at all. It is critical to understand and recognize the vulnerabilities detailed in this white paper and act quickly to fix them. Addressing these issues can help to prevent catastrophic data losses and will allow IT vendors to provide additional value for their customers while simultaneously protecting their reputations.

1. The Visible Ops Handbook

IT Process Institute's Visible Ops is a handbook designed to jumpstart implementation of controls and process improvement in IT organizations needing to increase service levels, decrease costs, and increase security and auditability.

http://www.itpi.org/the-visible-ops-handbook-review.html

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

1600 W. Broadway Road, Tempe AZ
(800) 804-6052
www.cleardata.com

ClearDATA
SECURE • HEALTHCARE • CLOUD