Kaseya® WHITE PAPER

HIPAA Compliance: IT Automation Makes It Almost Simple

14 Key HIPAA Tips for IT

Kaseya®

Ever since the Health Insurance Portability and Accountability Act of 1996 (HIPAA) debuted, small and medium-size healthcare organizations have been struggling to comply. And with new rules coming out with regularity, the process becomes more rigorous all the time.

Those knowing HIPAA could probably stand to learn a bit more – the rules are complex and subject to change. Those that don't know HIPAA are liable for some serious penalties and loss of reputation and business.

While HIPAA rules the roost in US healthcare, there are similar regulations the world over. And there is much more than just compliance to worry about. The reason for compliance in the first place is to safeguard your data. And these breaches are very real. As the Financial Times reported, one breach alone resulted in healthcare provider Anthem having records on 78.8 million patients compromised.

In fact, 23% of all breaches in the U.S. are against healthcare organizations, according to a study from the Brookings Institution. And in the last six years, these breaches have affected over 150 million Americans. The cost for each breached record is $363 – more than any other industry in U.S.

This white paper will walk through where HIPAA came from and why it emerged, and 14 things you need to know to stay in compliance – and safeguard your precious health data. We'll also explain how technology makes HIPAA compliance easier and feasible for even small and medium-sized healthcare organizations.

A Brief History of HIPAA

HIPAA has many purposes, including easing the transition for a consumer from one medical plan to another. More relevant is that HIPAA is largely designed to protect health and patient information, so-called protected health information (PHI), which means securing patient data at all times and all places.

The HIPAA Privacy Rule is the part that defines how PHI is shared, saved and accessed.

Meanwhile the HIPAA Security Rule created a legal infrastructure for electronic protected health information (ePHI) that defines how this information is created, transmitted and maintained.

Later in 2009, the supplemental Health Information Technology for Economic and Clinical Health (HITECH) passed. With this, the fines and penalties for non-HIPAA compliance increased to up to $1.5 million for each violation.

Things got even tighter in 2013, when the U.S. Department of Health and Human Services (HHS) passed the now famous omnibus ruling.

This ruling introduced the notion of Business Associates (BAs) with access to patient data by working with healthcare providers (known as Covered Entities). The issue here is that BAs became suddenly liable for compliance violations, as are all subcontractors. The same is true for hosters and backup providers who store medical data.

Who is covered by HIPAA?

- Health and Life Insurers
- Healthcare Providers
- Hospitals and Medical Facilities
- Public Health Organizations
- Colleges and Universities
- Business Associates
- And more

14 Things IT Should Know About HIPAA

1. Penalties are serious.

Huge healthcare operations all know HIPAA. They have to. They are the ones most impacted by the rules, and most likely to be subject to frequents audits.

Smaller operations don't always understand the full scope of the risk. But penalties are more than serious, even for these small organizations.

Here are just a few of the fines dished out in the U.S. in recent years:

- Affinity Health Plan paid $1.2 million because it didn't erase the drives on its advanced photocopiers before returning them to the company that leased them.
- WellPoint didn't secure an online health database and paid $1.7 million.
- The Massachusetts Eye and Ear Infirmary failed to encrypt physicians' laptops and was hit with a $1.5 million fine.
- Phoenix Cardiac Surgery posted patient appointments on an online calendar and paid $100,000.
- A Walgreens in Indiana breached a single patient's privacy, and paid her $1.44 million.
- An Idaho-based hospice lost a laptop due to theft. The fine was $50,000.
- A medical practice in Phoenix sent patient data over insecure email, and was fined $100,000.
- A pediatric practice in Massachusetts lost a flash drive and settled for a $150,000 fine.
- Another stolen laptop in Boston had the doctor paying $1 million.
- And the loss of a backup drive cost the Alaska State Health Department $1.7 million.

This is only scratching the surface. The HHS keeps an extensive list of violations.

2. Encryption is your friend.

HIPAA calls for all PHI data that is transmitted electronically to be protected, which is best done by strong encryption. In fact, if the data is strongly encrypted, organizations are pretty much immune from penalty if that data is somehow breached, or a lost device is already encrypted.

3. Many healthcare organizations don't care about HIPAA nearly as much as they should.

Very large hospitals and other big healthcare organizations invest many resources (both money and people) to address HIPAA regulations. They have the most to lose and are most in the prosecutorial cross hairs. And they can most afford to take HIPAA seriously, pay for the technology to support compliance, and train their workers.

Unfortunately many small and medium practices don't much care about HIPAA – they haven't been audited and don't expect to. They don't view HIPAA as a threat, don't worry about penalties, and don't see HIPAA spending as a priority – even if they had the extra cash.

However, a HIPAA fine could be financially devastating and ruin the trust between providers and patients – a real business crusher.

Smaller healthcare organizations are most in need of developing HIPAA expertise since they aren't closely aligned with large insurance companies and hospitals that have strong HIPAA controls in place.

4. Hosters have specific responsibilities.

Hosting companies must meet certain requirements. HIPAA requires that patient data in transit and stored must be secure and protected.

You should know that a HIPAA fine could be financially devastating and ruin the trust between you and your patients – a real business crusher.

Kaseya®

That means the hoster, to be HIPAA compliant, has to meet guidelines set by and judged by HHS.

Here are some things compliant hosting and compliant data centers must offer:

Physical security
This means there is limited access so only authorized people can enter the premises. Hosters also have to take extra care in how their workstations are protected, and PHI and ePHI data is transferred or ultimately disposed of.

Policies
The hoster must have technical policies that ensure the PHI and ePHI maintains total integrity and isn't altered or somehow deleted.

Storage
Backup and recovery must be strong, and support a true disaster recovery system so any patient information can be restored.

Access control and safeguards
Strong access controls must be in place to make sure only authorized users with HIPAA training can get to the data. This is done through user privileges, policies, and authentication.

Auditing
Hosters need to audit their HIPAA operations with full reports and log files to understand security problems and make sure they don't reoccur.

Network security
Hosters must guarantee their networks are fully secured, can't be accessed by unauthorized users and the data has encryption or some of other means in place so that the network can't be breached.

5. The security assessment is the first major step in HIPAA compliance.

Whether you are taking care of HIPAA compliance in house, or outsourcing, HIPAA requires a security assessment. This can start out broad, but needs to move to a deeper dive security assessment to define what needs to be changed immediately, what new technologies should be put in place, and how solutions such as end-user managment and authentication and access management can help achieve HIPAA compliance.

The assessment covers:

- Security policies relative to HIPAA
- An analysis of vulnerabilities, risks and system threats
- A plan for protecting and securing ePHI no matter where it is

6. It pays to document.

HIPAA rules require that healthcare companies and BAs must document the protective measures in place for ePHI. These documents must be given to all staff and they should understand what they mean.

7. Training is more than just a good idea. It's a must.

Training is about the core need to protect ePHI. End users, in and outside the main provider organization, must understand proper use of passwords, complexity and regularly creating new passwords. Organizations also need to know how to block and recover from malicious software. At the same time, organizations need expertise in logins and login monitoring and all relevant aspects of security.

You may believe that if you meet HIPAA rules, your organization is safe and secure. Far from the truth.

Kaseya®

8. Compliance is just one aspect of security.

You may believe that if you meet HIPAA rules, your organization is safe and secure. Far from the truth. As an IT pro, your job is to help achieve security and efficiency in all aspects of the business.

9. Encryption is a confusing aspect of the rules, but err on the side of caution anyway.

Encryption is one area where HIPAA isn't completely explicit. Instead the HHS talks about doing "what is reasonable and appropriate" to protect ePHI, and then says:

"In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification:

- Implement the addressable implementation specifications;
- Implement one or more alternative security measures to accomplish the same purpose;
- Not implement either an addressable implementation specification or an alternative"

This basically says the healthcare player or BA must find an effective way to secure data. One of the biggest issues is data in transit. Here the only way to know the data is protected is to strongly encrypt it.

So the answer is HIPAA doesn't specifically require encryption, but encryption is the only reasonable and viable way to meet HIPAA demands that ePHI be always protected.

10. You must have a security incident response plan (SIRP).

A SIRP details and documents what will be done in the case of security breach or other security event. Part of this is tracking security events, hopefully to prove no successful exploits have taken place. Just like running afoul of other rules, failure to properly respond to a security problem can draw a fine.

In the event of an attack or breach (even just an attempt), you should document what happened and the incident's severity. Attacks of organizations with more than 500 employees, patients or partners must be reported to the HHS.

Most importantly, follow the steps in the SIRP to stop the attack. That's what it's there for.

Finally, reevaluate your risk assessment in light of the new event.

11. A partner may be the best defense in the case of an audit.

An audit is when a healthcare organization is vetted to make sure it is in compliance. The aim is to define the state of the organization and see what steps are needed to improve performance.

These are supposed to be annual.

Most healthcare organizations, even large ones, are not equipped to handle an audit, with all its complexity. They need to evaluate their ability to handle an audit. Do they have real-time monitoring of key systems? Can they quickly and easily create reports that document network and system access? Can they prove their systems are secure? Can they document who has had access to which information? If so, they may be able to handle an audit as well as anyone. But, just as when the IRS comes knocking, they might want to pull in a partner.

"When it comes to surviving a HIPAA audit or data breach investigation, you need a professional. Like the specialists doctors refer patients to every day, and the tests that they order to see what is happening under a patient's skin, your technology must be evaluated by someone with the proper skills and experience, who must look deep into your network to identify its strengths and weaknesses. Make sure they understand the HIPAA compliance requirements you face," wrote Semel Consulting, a HIPAA firm.

Most healthcare organizations, even large ones, are not equipped to handle an audit, with all its complexity.

Kaseya®

12. Say no to Web e-mail and yes to firewalls.

Free Web e-mail is tempting. It's easy to set up, and messages can get sent from most any device.

But Web mail is a big HIPAA no-no. HIPAA demands e-mail that is secure from end-to-end, and backed by a vendor with whom there is a Business Associate Agreement (BAA).

Firewalls are also required, and these should be robust devices or services. Don't think this is a big issue? Neither did Idaho State University (ISU). The HSS found that medical records for 17,500 patients at ISU were not secure because the ISU firewalls were disabled for close to a year.

The fine? $400,000.

13. Access safeguards and controls require a new approach to authentication and access management.

One of the biggest issues, in fact the crux of the HIPAA matter, is making sure only those with the proper authority can access ePHI and the systems that contain it. Information access management policies and procedures are key to locking down unauthorized access to ePHI and other health data.

Mini access management checklist:

- How are authorized users given access, and how is this monitored and managed into the future?
- What is the policy and practice for modifying a user's access, such as blocking the user, changing privilege levels or changing what resources they can access?

14. HIPAA requires administrative safeguards.

Administrative safeguards are procedures and policies to make sure security violations or breaches don't occur. It also involves detecting incursions, containing attacks, and correcting problems.

Mini-administrative checklist:

- Have you completed a full risk analysis in compliance with HIPAA and National Institute of Standards and Technology (NIST) rules?
- Have you chosen a security official responsible for overseeing all these policies and keeping them updated?
- Have you defined how access reports, audit logs and incident tracking are handled?

A Bright Outlook

The good news is that healthcare organizations are increasing their budgets. According to a recent report from IDC Health Insights, "Business Strategy: Trends and Opportunities in the U.S. Healthcare Provider Market – A Discussion of the 2015-2016 Healthcare Provider Technology Spend Survey Results," healthcare spending by hospitals with over 200 beds is on the rise, with 40% of those polled saying budgets are growing.

This money is being spent wisely as much of it is going towards security – a key way to insure HIPAA compliance.

8 HIPAA Terms You Should Know

Covered Entities (CE)
Providers that offer healthcare treatment or services, and generally collect payment for them.

Business Associates (BA)
Partners that somehow have access this patient information. Business Associates (BAs) must be HIPAA savvy and remain always in compliance.

Electronic Protected Health Information (ePHI)
This is Protected Health Information (PHI), in electronic form. HIPAA covers PHI whether in paper or electronic form.

Healthcare Clearinghouse
These are organizations such as billing companies that handle health information and often transfer it to a standardized form or format for easier use.

Health Information Technology (HIT)
This is technology specifically designed for healthcare; it includes solutions meant to insure HIPPA compliance. For larger healthcare operations that handle their own IT, there may be a HIT administrator.

Due Diligence
When a healthcare organization is found in non-compliance, the answer isn't just a blanket penalty. Mitigating circumstances and the organization's behavior come into play. If the organization and its BAs have taken due diligence, the penalties are far less, perhaps just $100 for each incident.

Reasonable Cause
Here, like due diligence, the organization has acted in good faith. When it comes to reasonable cause, in most cases steps have been taken to meet regulations, but an area to insure compliance is missing or not addressed. Fines here are a minimum of $1,000 per incident, and usually less than the $50,000 maximum. Repeated incidents can be fined at a far higher rate.

Willful Neglect
In the case of a violation, willful neglect is a worst-case scenario. If an organization is found to exhibit willful neglect by ignoring HIPAA, but corrects the issue, the fines start at $10,000 per incident.

If the organization doesn't correct its error, minimum fines start at $50,000 per incident and quintuple for repeat offenses.

Kaseya®

This includes:

- Understanding and controlling Shadow IT, where individual or departments implement their own technology, and which can compromise the network and compliance. These rogue projects can be unearthed and controlled with network monitoring, software inventories, and audits.
- Cloud security is critical as data in the cloud can be harder to protect than information that stays exclusively in house.
- Systems and network monitoring is essential to knowing what is happening within an organization's data, especially who is accessing what. This information is critical in the case of a compliance violation or audit.

And IDC Health Insights predicts that by 2020, the vast majority of healthcare data, some 80%, will move across the cloud. This means all this data must be professionally secured, managed and audited. This in general requires a HIPAA compliant cloud provider, proper monitoring, and insuring the data is secure and protected before it moves across the cloud.

6 Things to do Right Away

Think about your hardware
There are some elementary things a healthcare organization should do first. For one, the PCs themselves. These should be modern so the operating systems are fully supported with updates and security patches. And don't cheap out on the OS. In the case of Windows, the Professional and Enterprise versions are far more secure than consumer revs, such as allowing for more secure network connections.

Bone up on security training
Staff must be expert in all relevant HIPAA rules, especially as they pertain to specific job functions. At the same time, organizations need to be prepared to train the staff for any BAs.

Create an asset disposal plan
PCs turn over quickly as they break, lose performance or can't run new software. The same can't be said for the data which can last forever. A HIPAA overseer's duty is to help dispose of devices safely, and make sure absolutely no data can be recovered.

Have a Business Continuity/Disaster Recovery plan
Keeping prying eyes away from health data is one aspect of HIPAA. But there is another form of data protection – making sure the data is available in the event of trouble. Organizations must have a recovery plan that defines how disasters are handled and business continuity maintained.

Keep Business Associate Agreements (BAA) at the ready
In order for a partner to help with HIPAA work, there must be a BAA contract firmly in hand. As the relationship with a partner moves forward, reach new agreements that account for these changes. These agreements cover both what both parties are responsible for.

Produce a comprehensive antivirus/anti-malware policy, and be prepared to implement it
This comprehensive policy needs to analyze what protections are in place, what new ones are needed, and steps to take in the event of an attack or incursion.

The Technology Answer

These days there is plenty of technology to make organizations of all sizes secure and compliant – and ready to defend itself in the case of a HIPPA incident. PCs and servers need to be protected from viruses and malware. That involves good antivirus and anti-malware tools, but also the ability to discover all the devices that need protection and easily install security software. At the same time, all machines need to be up-to-date in terms of patches and software updates, a job best handled by an automated solution mated with network and device discovery.

Additionally, access to device and files need to be carefully controlled through policies and solid password management. And as a defense if an organization runs afoul of HIPAA, it is best to track who has access to what and when – and to have this all in one easy-to-digest report.

Kaseya and Key HIPAA Questions

A Kaseya blog walked through key HIPAA questions to ask, including, the blog said:

- Are your employees aware of the penalties that will ensue from security violations?
- Are internal penalties in place for employees who violate security procedures?
- Do all your users know what to do in the event of security incidents or issues?
- Is there a process in place to document, track, and address security issues or incidents?
- Is there someone tasked with checking all security logs, reports, and records?
- Do you have a security official in charge of a password and smart security policy?
- Have you ever undertaken a risk analysis?

Kaseya®

Kaseya and HIPAA Compliance

As you can see, being a successful HIPAA compliant healthcare provider takes a lot of work, study, and a large dose of the right technology.

You need a comprehensive endpoint management platform to make it all possible. Kaseya VSA is that platform – and at a surprisingly affordable price. With it you can:

- Discover, audit, inventory and monitor every system and software component, with all operational details
- Simplify and automate patches management, based on your predefined patch policies and schedules to minimize network impact
- Access and manage computers from anywhere at near instantaneous connect times with extraordinary reliability, even over high latency networks
- Deploy policy-based automation with proactive remediation, to increase productivity and allow you to do more with your existing staff
- Gain insights into CPU, disk, memory, network bandwidth, files, logs and more - all from a single integrated console

Learn more about Kaseya or sign up for your free trial.

Then find out more about IT automation and HIPAA compliance with Kaseya's "Healthcare IT Systems Management: Challenges and Solutions" brief which you can **read here**.

Kaseya AuthAnvil Access Management and Authentication

Controlling who has access to data can go a long way in being HIPAA compliant. Single Sign-On (SSO) and Multi Factor Authentication (MFA) are key tools in keeping a lid on access to confidential information.

MFA, for instance, means that an end user validates their identity multiple ways, such as a fingerprint, or a piece of information only that user would know. This type of access management and control is essential to keep IT systems in HIPAA compliance.

Kaseya AuthAnvil is an industry-leading Identity and Access Management (IAM) solution, and makes meeting audit and compliance requirements easier and simpler. In addition to SSO and MFA, AuthAnvil allows you to track all activity, know the health of your passwords and be informed when they are at risk of non-compliance. In addition, with powerful reporting analytics to monitor permissions, can monitor permissions and for changes to ensure settings meet policy requirements.

Here are a few links you may find helpful.

For a HIPAA security checklist: **Click Here**

To learn about Kaseya AuthAnvil Multi Factor Authentication: **Click Here**

For details on Kaseya AuthAnvil Single Sign-On: **Click Here**

ABOUT KASEYA

Kaseya® is the leading provider of complete IT management solutions for Managed Service Providers and small to midsized businesses. Kaseya allows organizations to efficiently manage and secure IT in order to drive IT service and business success. Offered as both an industry-leading cloud solution and on-premise software, Kaseya solutions empower businesses to command all of IT centrally, manage remote and distributed environments with ease, and automate across IT management functions. Kaseya solutions currently manage over 10 million endpoints worldwide and are in use by customers in a wide variety of industries, including retail, manufacturing, healthcare, education, government, media, technology, finance, and more. Kaseya, headquartered in Dublin, Ireland is privately held with a presence in over 20 countries. To learn more, please visit **www.kaseya.com**

Rev 052516

Kaseya®