STORAGECRAFT
RECOVER-ABILITY™
GUIDES

MSPs and Healthcare: How to Be a HIPAA Compliance Hero

How understanding HIPAA can lead to increased profit, more clients, and a more capable workforce

By Casey Morgan

If you read anything about healthcare you'll know the hot industry topics are the Health Insurance Portability and Accountability Act (HIPAA), which regulates how healthcare providers (Covered Entities) and their business associates should handle electronic protected health information (ePHI), and a newer regulation, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which expanded the requirements set forth by HIPAA.

Many managed service providers (MSPs) see HIPAA as a regulatory nightmare. Some IT providers completely avoid any industry with regulatory compliance obligations, not just healthcare. And there's no wonder when a lot of what you read about regulations isn't that they're easy to deal with, it's that they can be complicated and frustrating, or that working in compliance-heavy industries ultimately isn't profitable.

But that's not the real story.

This informational guide[1] is designed to help you understand that despite the complexities of HIPAA, it's more manageable than it may seem. As an IT provider, you can be a valuable resource for Covered Entities subject to HIPAA, which can lead you to higher profits and the opportunity to work within other industries that have compliance standards.

Once you understand HIPAA, you'll likely see higher profits for your business, a workforce with better skillsets, and more potential work for your growing business—you might even end up with more secure networks at your own business.

1 This material is for informational purposes only and not for the purpose of providing legal advice. You must consult your own experts and attorneys to discuss HIPAA compliance obligations.

What is HIPAA, Really?

There's actually quite a bit to understand when it comes to HIPAA—more than we have space for here. Instead of detailing every little requirement, we'll cover some comprehensive information that will better acquaint you with understanding HIPAA and its importance. To summarize, and most relevant to MSPs, HIPAA is a federal law that requires Covered Entities and their business associates to safeguard the confidentiality, integrity, and availability of all electronic protected health information (ePHI) they create, receive, maintain, or transmit in compliance with HIPAA security standards (HIPAAs Security Rule).

Ultimately, it's about protecting sensitive medical information and moving on a reasonable, responsible path toward comprehensive information security. This means Covered Entities have to understand everything from where ePHI is stored and how it's transmitted to who has access to it (and when and where it's accessed), all the way to what types of security measures (both onsite at the healthcare facility and within their IT network) prevent attackers from stealing data.

Thinking about the real value of managed services for healthcare

Keeping people hale and hearty is priority one for the healthcare industry, and though your focus is on HIPAA compliance, it's not the only valuable aspect of your service. Having a better understanding of HIPPA obligations positions you as a HIPAA and technology advisor within an industry in which IT needs are increasing. Covered Entities don't typically have time to worry about whether their systems will work, and so your goal—and the true value in what you do—is making sure they never have to.

Your job is to help them identify and fix the risks, but you can offer a lot more to healthcare providers. Help them meet compliance standards, but remember that you'll be in the most profitable position if you help them with everything on the information technology spectrum as well, not just with what HIPAA mandates.

Understanding what HIPAA can do for you

We've briefly talked about what HIPAA is and about what you can provide as an IT professional, but what is your company getting out of this? Before you jump into any new industry, you'll want to know if it's really worth it. With healthcare, there are several benefits to consider.

Profit potential

StorageCraft® recently surveyed more than a hundred of our partners who work with clients in the healthcare industry. Results showed that 91 percent of respondents said there are monetary benefits for IT providers capable of handling HIPAA compliance for clients. There is plenty of profit potential because you'll be providing more than just tech support; you'll be providing security, uptime, and resources to assist Covered Entities meet their HIPAA-compliance obligations.

Increased client loyalty

We talked to our partner, Guy Baroan, owner of IT managed services company Baroan Technologies, about HIPAA. Guy works with multiple clients in the healthcare industry. According to Guy, it's beneficial to work with clients who are subject to HIPAA requirements because you can be very involved with their businesses. The more involvement you have, the more trust you can build with clients (plus you'll encounter more opportunities to offer billable services). As Guy says,

"With healthcare, you're really involved in building their business systems for everything. You're one on one with managers and owners and discussing what you're going to do to [help] meet requirements—you're the ultimate trusted advisor."

There are a few different ways you can approach HIPAA with your clients, but the one of the best ways for an MSP business involves handling as much of their technology needs as possible. "HIPAA is a huge opportunity for the IT industry—[a large percentage] of HIPAA compliance is technology," says Guy, and he's right. You can be the technology resource for HIPAA.

A leg up

If you don't become a HIPAA resource, your competitors might. Some Covered Entities aren't up to date on the latest HIPAA requirements, which makes now a great time to get started. In fact, a survey by NueMD revealed that 64 percent of Covered Entities weren't aware of recent HIPAA updates, and 32 percent were not aware that audits are happening. Their ignorance can create opportunity for you. As Guy says,

"[Healthcare providers] are hearing about HIPAA but they don't know all that's involved. It's an opportunity like nothing before—especially in the healthcare industry. If you're going in as an expert, you've got a leg up on others."

Not all MSPs are on the HIPAA bandwagon yet. Being ready to deal with HIPAA as soon as possible puts you ahead of competitors, and positions you as an excellent resource for Covered Entities that don't know what's involved in HIPAA compliance or haven't yet achieved HIPAA compliance.

Baroan Technologies

http://baroan.com/

Baroan Technologies is a New Jersery-based managed service provider with a mission to help small and medium businesses succeed by facilitating the best and highest use of information technology. Their "One Point of Contact" service delivery system for consulting, implementation, and support provides them the consistent and effective results they themselves would want as business owners.

A more secure business

We'll get to business associate agreements later in this guide, but it's worth noting that businesses who perform functions or activities on behalf of, or provides certain services to a Covered Entity are considered a "business associate" under HIPAA and are subject to HIPPA regulations as well—that includes your business. As you go through the compliance process your networks and processes will likely improve, which can ultimately improve your operations and strengthen your network security practices.

More capable employees

Your employees will gain knowledge about healthcare industry best practices as well as security standards and protocols that they may not have been aware of. These are skills that will help them in their careers, which in turn helps your business. Plus, understanding compliance in one of the toughest industries might just make it easier to provide support for other compliance-heavy industries such as the finance industry.

Referrals

Word of mouth goes a long way. If you do a great job assisting Covered Entities, you might start getting referrals from your happy clients. Wouldn't it be nice to be known as the company that solves IT problems for healthcare? That type of reputation isn't out of reach.

So don't think of HIPAA as a big regulatory mess. Think of it as your gateway to helping small businesses provide critical healthcare services to more people, while making them more secure in the process. Even though most of what you'll do involves providing businesses with technology resources, another big part is helping practices avoid penalties for non-compliance.

Being the HIPAA Hero

Your understanding of the risks will help you have discussions about HIPAA compliance with Covered Entities that either know they need to be compliant but don't know where to start or want nothing to do with HIPAA at all (yes, they're out there). Just remember, you won't be trying to scare healthcare providers into buying services, you'll be informing them so you can eliminate their risks and empower them with technology.

As we've explored, the goal of HIPAA is to prevent things like a data breach, which includes preventing unauthorized access, taking, and disclosure of ePHI. Data breaches, on average, cost $201 for a single lost or stolen record. A single stolen record may not seem that costly, but an entire breach event can be far more costly, depending on how many clients were affected and how many records were breached.

Covered Entities that do suffer a breach are likely to be audited, which can result in fines between $200K on the low end and up to millions on the high end (the US Department of Health and Human Services even keeps a running list of Covered Entities that have been forced to pay settlements).

And while healthcare providers are being audited, the audits seem to be relatively few. In fact, in our HIPAA survey, 72 percent said they have not worked with a client that's been audited, which suggests that the majority of providers haven't been audited—yet.

Some Covered Entities might be afraid of HIPAA fines and audits—it sounds scary. But since such a large portion of HIPAA involves IT specifically, an IT provider can ease their fear and be their HIPAA compliance hero.

But to truly be the hero, you have to learn all you can about HIPAA, and that involves meeting HIPAA compliance obligations yourself.

Becoming HIPAA compliant

The question you might have is why would you need to be HIPAA compliant when you're not the medical practice? Under HIPAA, each Covered Entity is required to sign a business associate agreement (BAA) with vendors or contractors they work with and which will have access to protected health information. Basically, in order for the Covered Entity to be HIPAA compliant, they must ensure that vendors performing functions or activities on their behalf, or providing certain services to them (e.g. your business) are also complying with HIPAA obligations. It may sound tough, but there's really no better way to understand how to help your clients become compliant than to become compliant yourself.

There are usually two ways providers will do it. Bear in mind that you'll want to make the compliance process easy for new clients who have HIPAA needs. As you become compliant, think about what you can do to make compliance changes smooth for clients. The goal here is to help others, so taking careful notes about the process will serve you well once you start working with healthcare providers.

Teaching yourself about HIPAA compliance

The U.S. Department of Health & Human Services' Office for Civil Rights is responsible for enforcing HIPAA, but all the information you need regarding HIPAA is available on the Department of Health and Human Services' website at HHS.gov.

According to Guy, this self-taught strategy of understanding HIPAA and its obligations requires a lot more work but can ultimately lead to HIPAA compliance at little to no cost to your company (other than time, effort, and any technology upgrades, if needed). But as he explains, it can be tough:

"If someone wants to spend the time, he can go to HHS.gov and read all the laws and regulations related to what they have to be aware of. This helps them understand both what a business associate needs to know and what the medical practices themselves need to know in order to be compliant. That site also has links to more resources, samples, templates, documents, BAAs you can use—they've got everything on that site."

for testing methods, these are some ways you can test your backups so you and your clients know recovery isn't just a nice thought—it's a guarantee.

Learning HIPAA compliance with third parties

If doing all of the work yourself sounds too hard, third parties can help out with HIPAA and they all offer various benefits for various fees. According to our HIPAA survey, only 30 percent of those surveyed use a third party to help them with HIPAA compliance, but that's not to say they aren't beneficial.

Some third parties offer classes and certifications (such as CompTIA). Others specialize in HIPAA compliance from top to bottom. Guy uses one that helps him cover all his bases and says that since the HHS.gov has an overwhelming amount of information, a third party can be invaluable.

Third party services often help you with a self-test that lets you identify your risks so you can eliminate them. They can also keep you in the loop on the latest updates to compliance requirements while also storing your HIPAA-related documents (policies, procedures, breach plans, etc.) in one place. Guy says,

"Basically they take all the information from the HHS website and put together a portal for businesses, medical practices, IT firms, or anybody who is a business associate, and they help them become HIPAA compliant by doing all the back-end work for you."

These companies will walk you through what needs to happen for compliance, such as risk assessments, required documentation, and so forth. Since many of them keep all of your documents in one place, it's easy to show new clients your compliance program, which is something any savvy Covered Entity will look for.

The other benefit of working with a third party is that many help you assist your clients in becoming HIPAA compliant.

Note, however, that there are varying levels of quality and pricing when it comes to these third parties. You'll want to vet these companies carefully when it comes to something crucial like HIPAA.

Assessing and Updating

Once you've become compliant yourself, you'll be ready to start helping others be compliant. The first stage is conducting a risk assessment, which reveals any vulnerability a client might have with regard to technology and processes. Sometimes these lists of vulnerabilities seem long, but your job is to work through the list and better secure your client's IT infrastructure.

The trouble, of course, is that implementing new backup and recovery procedures (see "How StorageCraft Recover-Ability™ Helps"), security features, and processes costs money for a Covered Entity. Many Covered Entities understand the value in HIPAA and that you are there to help them navigate the issues, but these aren't the ones to worry about. There's another class of healthcare professionals who don't think HIPAA affects them at all.

Our HIPAA survey revealed that only 24 percent of our partners said that all of their clients in the health field were worried about HIPAA. That means 76 percent of them have a number of clients who are not concerned about HIPAA. So what do you do with these people?

Addressing reluctant clients

Despite the fact that penalties, including fines and fees for non-compliance, can potentially crush a small practice, healthcare providers aren't always on board with HIPAA. Some even say they flat-out don't care about it and assume that because they're a small practice, HIPAA won't affect them.

This is silly, of course, when you see that several small practices have been penalized and/or fined. A small practice owned by two physicians was fined $100K in 2012, and another small dermatology practice was fined $150K in 2013. Size and specific medical focus don't seem to be factors when it comes to investigations—it can happen to any healthcare provider.

You can try to reason with reluctant clients, but you may need to consider other options. Our survey found that some IT providers suggested trying to convince them of the need for HIPAA (56 percent), some suggested having the practice sign special agreements (27 percent), and some suggested just refusing to work with these clients (26 percent).

If you have reluctant healthcare providers, make them aware of:

- The fact that audits are happening now
- The fact that healthcare providers have and continue to be fined for non-compliance
- The potentially high cost of non-compliance
- The irreparable damage to their reputation should a data breach occur
- The potential for legal action on the part of clients whose data is lost or compromised
- The fact that size of practice and their specific healthcare focus won't be saving factors

The bottom line is that it's not worth the risk for a Covered Entity to be out of compliance. If you've tried reasoning with them and they're still hesitant, this may not be a client you want to work with.

In summary

Whether you elect to teach yourself about HIPAA or work with a third party, HIPAA compliance is a valuable compliance standard to be familiar with. Understanding how to deal with HIPAA will take work, but as we've noted, the rewards are numerous. It pays to take the time to understand these new regulations and to be on top of them. There's no better time than now, and if you're looking for new industries to break into, healthcare is a great one to work toward.

How StorageCraft Recover-Ability Helps with HIPAA Compliance

As discussed, HIPAA requires Covered Entities and their business associates to ensure the confidentiality, integrity, and availability of all electronic protected health information (ePHI) they create, receive, maintain, or transmit in compliance with HIPAA security standards.

StorageCraft Recover-Ability, can help Covered Entities and their business associates meet their HIPAA-compliance obligations.

HIPAA's Security Rule likely applies to the data backup and disaster recovery services StorageCraft offers. The Security Rule is intended to maintain confidentiality of ePHI, protect it from improper modification or deletion, and ensure that ePHI is available to authorized persons when needed. It requires that Covered Entities have appropriate administrative procedures, physical safeguards, and technical safeguards to protect and secure ePHI. Below is a sampling of those requirements and how StorageCraft Recover-Ability addresses them.

- Administrative Procedures. Covered Entities must have a meaningful data backup and disaster recovery plan. CFR 164.308. This includes establishing and implementing procedures to create and maintain retrievable exact copies of electronic protected health information, procedures to restore any loss of data, procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode, and procedures for periodic testing and revision of contingency plans.
- Physical Safeguards. Covered Entities must limit physical access to their information systems and the facilities in which they are housed. CFR 164.310.
- Technical Safeguards. Covered Entities must implement safeguards to ensure encryption of ePHI at rest and in motion. CFR 164.312.

How StorageCraft Recover-Ability address the Security Rule's Administrative Procedures

StorageCraft Recover-Ability facilitates compliance with the Administrative Procedures requirement through StorageCraft's industry-leading protection and security measures used to secure user data. With image-based backups taken with StorageCraft ShadowProtect® and StorageCraft ShadowProtect SPX, you can back up any critical system entirely. With ShadowProtect and SPX, you can quickly retrieve data through simple file and folder recovery, or through a full system restore—either using locally stored backups, backups saved remotely via StorageCraft Cloud Services™, or at your own datacenter or a co-location facility.

- Pre-stage recoveries using our patented StorageCraft HeadStart Restore® technology for quick recovery.
- Implement full restores to dissimilar hardware using our StorageCraft Hardware Independent Restore™ technology.
- Spin up a virtual machine of critical systems in minutes using StorageCraft VirtualBoot™ technology.
- Virtualize a machine or network via StorageCraft Cloud Services™.

Our ebook Making Disaster Recovery Easy covers nearly everything you need to know about recovery.

Backup and Recovery Testing

To help meet the periodic testing requirement, you need to test your disaster recovery plan and verify that your backups can be restored. StorageCraft Recover-Ability gives you several testing options that range from quick and simple to advanced and all-encompassing:

Automatic verification. By setting up automatic verification of backup images using StorageCraft ImageManager, you'll know that backups are valid without a hands-on test.

File and folder restore. By mounting a backup as an NTFS drive letter, you can browse and restore files and folders in minutes. This lets you validate the integrity of a backup and the files therein.

Virtual machine. By spinning up a backup as a virtual machine using StorageCraft VirtualBoot technology, you can verify that the backup image can boot properly. Once running, you can browse the system as it was at the exact moment you took the backup.

Full restore. By using StorageCraft Hardware Independent Restore™ technology, you can test a backup by implementing a full restore on secondary hardware. This will allow you to verify that not only will the backup work as a VM, it will also function properly as a physical machine, and even on dissimilar hardware.

Cloud recovery. By using StorageCraft Cloud Services, you can retrieve files and folders from backups stored in the Cloud or to run a full system as a VM from the Cloud. This process takes mere minutes.

Our ebook Don't Let a Disaster Be Your First Backup Test reviews the benefits of these testing methods in detail.

How StorageCraft Recover-Ability Addresses the Security Rule's Physical Safeguards

StorageCraft Recover-Ability facilitates compliance with the Security Rule's physical safeguards by using Tier 3 and Tier 3+ datacenters. These data centers assist Covered Entities in meeting the Physical Safeguards requirement because they are provisioned with security systems, video monitoring systems, man-traps, card-key systems, and 24x7 on-site security which "limit[s] physical access to [] electronic information systems and the facility…in which they are housed." CFR 164.310(a)(1).

How StorageCraft Recover-Ability Addresses the Security Rule's Technical Safeguards

Finally, the Security Rule's third requirement is that a Covered Entity implements reasonable Technical Safeguards. StorageCraft Recover-Ability helps its customers meet this requirement. For example, StorageCraft Cloud Services helps to "guard against unauthorized access to electronic protected health information that is being transmitted" by employing unique user identification controls, strict logical system access controls, data encryption[1] at rest and in

1 It is the responsibility of the end user to encrypt the source data to meet compliance with their specific HIPAA obligations. StorageCraft Cloud Services will not accept data unless such data has been encrypted.

A Brief Conclusion

Summary

While StorageCraft Recover-Ability can assist Covered Entities and business associates in complying with HIPAA including the Administrative Procedures, Physical Safeguards, and Technical Safeguards requirements of the HIPAA Security Rule—StorageCraft products and services form only one piece of overall HIPAA compliance. In other words, StorageCraft can offer assurances about the technical security of data through measures like encryption, physical security, and redundancy, but you (as a business associate) and Covered Entities you assist, must ensure that you understand the requirements for handling ePHI, adopt appropriate policies and procedures, and follow those policies and procedures. If Covered Entities and their business associates don't have polices in place to control access to their specific data, then even the most technically secure environment cannot ensure that ePHI will not be compromised.

For more information about HIPAA and the Security Rule, go to the U.S. Department of Health & Human Services web site.

This material is for informational purposes only and not for the purpose of providing legal advice. You must consult your own experts and attorneys to perform a HIPAA compliance assessment. This informational document does not alter or amend the terms and conditions of any agreement you have with StorageCraft, including the Cloud Services Agreement.

About the Author

Casey Morgan is the senior marketing content specialist at StorageCraft, a U of U graduate, and an Oxford comma enthusiast. Casey has spent the last few years writing hundreds of pieces of marketing content—from infographics to ebooks, blog articles, and web copy. He believes that content isn't just about selling products, it's about connecting and empowering people and businesses. When he's weary of words, you might find him and his dog in the woods or enjoying a cool homebrew.

StorageCraft Technology Corporation
11850 S. Election Road, Suite 100
Draper, UT 84020

www.StorageCraft.com
1.801.545.4700
contactus@storagecraft.com