HIPAA®
SECURITY SUITE

Your key to HIPAA compliance®

An Acentec, Inc. Solution

The Ultimate HIPAA Compliance Handbook

Acentec
Improving Medical Practice Performance®

HIPAA Security Suite is an Acentec, Inc. Solution

Contents

Contents

HIPAA Basics

HIPAA Basics

The Omnibus rule of 2013 was a game-changer for HIPAA. Among the many changes it ushered in, it included a new penalty and enforcement structure that put a considerable bite into the law. Understanding what's required of a healthcare organization, or other industry participants can be challenging and expensive. There are a few basic principles that can take some of the complexity out of becoming and maintaining HIPAA compliance.

Understanding the THREE Pillars of Compliance

HIPAA has traditionally been broken down into the Privacy Law and the Security Law. The Privacy Law addresses patient rights and patient privacy, while the Security Law addresses protecting the organization and its data. Many organizations have their compliance efforts divided along those lines – they'll have a Security Compliance Officer and a Privacy Compliance Officer. While that is an effective approach, the Omnibus Rule, in an effort to more closely align the laws governing HIPAA, blurs the lines between those previously clean distinctions. Today, HIPAA can be approached as a single body of law, requiring different disciplines for compliance, but with the previously disparate pieces now overlapping each other.

To reflect that paradigm shift, we break HIPAA compliance into three specific parts, or what we call the Three Pillars of HIPAA Compliance. Those three pillars are Training, the Risk Assessment, and Policies and Procedures. Critical to this approach is the understanding that all three parts are inter-related. In other words, the findings of the Risk Assessment must reflect what your Policies and Procedures state, and your Training needs to reflect your Policies and Procedures.

Accomplishing this can be difficult when different vendors are providing different areas of compliance – your training company is different than whom you're using for your policies, and your risk assessment, etc. This causes one of the more common comments we hear in OCR corrective action memorandums – the organization failed to follow its policies and procedures. When conducting risk assessments for our clients, we frequently identify practices being used by staff that, while they may be HIPAA compliant, contradict what was documented in their policies.

What it means to be HIPAA Compliant

Rarely do we speak with someone in healthcare who, when asked if they're HIPAA compliant, provides an accurate answer. In almost all cases the answer to that question is yes. And I believe they are being genuine, they honestly believe they are compliant. But it's not until we ask additional questions that we mutually discover some gaps that need to be filled. For a list of questions to ask yourself, you can download it here.

In this chapter, we're going to dig in a bit deeper into the Three Pillars of HIPAA Compliance.

Policies and Procedures

Your policies and procedures are the lynchpins of your compliance efforts. Here is where you document how your organization operates. Your policies need to be current, implemented, integrated, trained, and available to everyone.

There are two components to keeping your policies current. First is ensuring your policies reflect the actual procedures in practice at your organization. Since these change over time, your policies need to be reviewed regularly to be accurate. In addition to regular reviews, at times new policies need to be added. For example, most organizations now have policies for mobile device use on their premises and also a social media policy. You may not have had either of those policies just a few years ago. In fact, not only should you have a social media policy, but you should have two – one that states how your organization engages in social media (or not), and two, the responsibilities of your workforce regarding social media.

Implementing your policies and procedures means your workforce understands what they are (because they have been trained on them), and adheres to the documented policy. As stated previously, having practices that differ from your policy is a potential HIPAA violation that could result in penalties.

On the subject of documenting your policies, many of our clients, when asked if they have a backup policy, for example, will tell us what they do for backups. When we ask if they have it in writing, well, you can guess the answer. Knowing how things get done in your organization is not enough, and it's not HIPAA compliant unless it's documented.

What it means to be HIPAA Compliant

Along the same lines as having practices that reflect your documented policies, those also need to follow through to the findings in your Risk Assessment and the training your staff is getting. That integration is critical to having a cohesive compliance strategy. Ideally, your policies state exactly how your organization operates, your Risk Assessment reflects those findings, and your workforce is trained on your organizational policies. Achieve this, and your operation is running in harmony; your organization is more resilient to turnover, and it's less vulnerable to existing risks, cyber and otherwise.

Training

Workforce errors are the leading cause of HIPAA violations. Errors in this context include clicking malicious email links or opening infected email attachments. We should also add the accidental sharing of network access credentials since this is as well a major target of hacker's efforts.

Training is a perfect example of where meeting HIPAA compliance doesn't come close to improving your cybersecurity posture. HIPAA requires workforce training to be conducted at least annually while best practice recommendations go on to encourage regular reminders and reinforcement. In today's rapidly changing cyber risk environment, this simply isn't adequate. Workforce HIPAA and cyber-awareness training need to be almost constant. Your organization should make it part of your culture. The trainings doesn't have to be lengthy or time- consuming, but rather consistent and frequent. An example of this would be Acentec's HIPAA Reminder Emails. These free, weekly reminders meet Section 164.308(a)(5) of the HIPAA Security Rule and help to keep HIPAA and cybersecurity at the forefront of your workforce's minds.

Finally, your training also needs to be integrated with your policies and procedures. If you're training your workforce on certain practices, but those practices don't reflect what's documented in your policies and procedures, then you're vulnerable to a HIPAA penalty. This is another reason why a comprehensive solution to HIPAA compliance is superior to attempting to meet the Three Pillars of Compliance with different vendors.

Risk Assessment Report

The Risk Assessment is the most powerful tool you have to identify how your organization is operating from a HIPAA compliance perspective. Many people assume the risk assessment, or security risk assessment, is a technical exercise to be conducted by IT personnel. While the technical aspect of a risk assessment is important, it is not the only metric that needs analyzing. A proper Risk Assessment will evaluate the following criteria:

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards
- Organizational Requirements
- Policies, Procedures, and Documentation Requirements

Each category has its own set of metrics to evaluate. It's beyond the scope of this book to delve into the details of each one, but NIST, the National Institute for Standards and Technology, provides an excellent framework as a guide for conducting a proper risk assessment. The point I'm making here is a risk assessment traverses the entire organization and is not confined to the technical aspects of your business. Here again, your risk assessment should be a cohesive process that results in a unified course of action and not a disjointed and disconnected compilation of reports from your different departments.

Lastly, as I mentioned before, we often get caught in the trap of striving to achieve compliance without sight of the real goal of all of this. The risk assessment should be a living document that's updated as circumstances change, which they do frequently. Switching from local Microsoft Office to Office365, for example, is an event that should be chronicled and documented in your risk assessment. Likewise would be replacing hardware or adding a new medical device. Waiting for your next assessment to be conducted to update an event like this isn't proper. Likewise, your policies should be updated at the time of transition so they accurately reflect your then-current environment. This is what we mean when we talk about all of the parts of a HIPAA compliance process being inter-related.

What it means to be HIPAA Compliant

Speaking of your next assessment, let's consider the actual verbiage in the HIPAA law

> § 164.308(a)(1)(ii)(A) - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronically protected health information held by the covered entity.

Notice the absence of a specific timeframe. Don't let this fool you. In later subsections, it clearly states aspects of the risk assessment must be conducted regularly. But the most telling sign on frequency can be found in the OCR's Corrective Actions documents. Whenever a Covered Entity is found to have a risk assessment that is older than a year, they are cited for failing to keep an updated assessment. For the reasons stated above, our company policy is a risk assessment should be conducted at least annually and updated as circumstances dictate.

Remediation Plan

Congratulations! Your team and your vendor have completed your risk assessment. Before you take your lovely report and file it away, you need to address its findings. Very few organizations reach the final stage of the assessment with no identified shortfalls. These gaps in compliance have to be addressed, and that's where your Remediation Plan comes in.

A Remediation Plan is a written, or online, document that lists the weaknesses in your organization as they were identified during the risk assessment, and states courses of action to address those concerns. A remediation plan MUST also include estimated dates of completion as part of this process. Some remediation plans allow for interaction that includes being able to assign specific tasks to other users or parties and then track what has been completed and what is still outstanding. Ideally, a remediation plan will alert you if a task is due to have been completed, but has not been checked off yet.

Beyond the documentation is the remediation itself. While larger organizations often have the staff, expertise, and resources to conduct their remediation, many others aren't as well equipped. Finding a good third party to work with on this process can be a cost-effective alternative to attempting the project internally.

What it means to be HIPAA Compliant

Regardless of how you approach resolving remediation plan issues, it's a vital part of your HIPAA compliance and the overall security of your organization. Leaving known shortfalls unaddressed could expose you to the classification of being "willfully negligent" by OCR and potentially your liability insurance carrier. Such a designation may leave you out in the cold to face fines, penalties, and lawsuits with no protective cover. Don't get caught in that situation.

Staying HIPAA Compliant

One of the most frustrating aspects of running a compliance company is to leave an engagement with a client with a mutual understanding of what needs to be accomplished to reach HIPAA compliance, only to find out, on our next visit, for example, the organization had reverted to the risky (and non-compliant) ways of the past. Here's a mantra all Covered Entities should chant – HIPAA compliance is not a destination to be reached, but rather a goal to maintain. It is not a one time or annual achievement that is completed in a vacuum, or the secrecy of the executive offices. Maintaining HIPAA compliance requires a consistent vigil from the entire organization. We call it "culturalization". HIPAA compliance, and for us, we include cybersecurity awareness, needs to become part of the daily behaviors and thoughts of everyone in the workforce. It cannot be perceived as someone else's responsibility, or "that's handled by another department". Every workforce member holds the keys to the castle, and one momentary lapse can invite havoc and destruction into the organization.

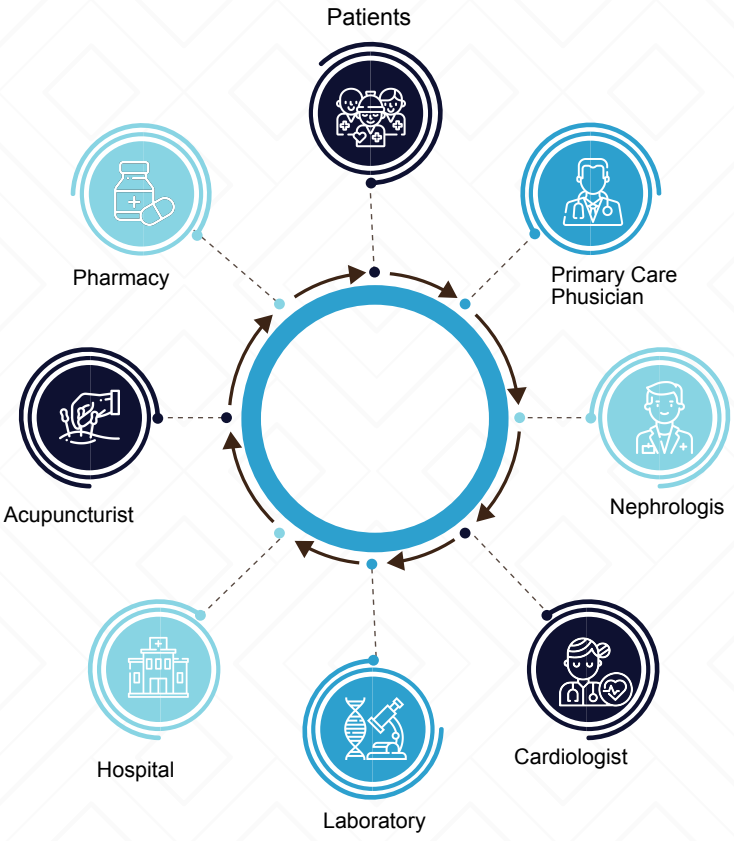
Achieve compliance, maintain compliance. These are your goals with HIPAA.

The Gap Between HIPAA Compliance and Cybersecurity

The Gap Between HIPAA Compliance and Cybersecurity

A gap does indeed exist between HIPAA requirements and cybersecurity recommendations. For entities who aren't bound by HIPAA, they can lock down their infrastructures as tight as they want and the only backlash they face are complaints from a disgruntled workforce. The same is not true for the healthcare industry. As healthcare professionals, you've been forced to confront an almost untenable dilemma. You are mandated to secure Protected Health Information (PHI) while at the same time you are mandated to share it. What's worse, OCR has made it known they intend to enforce penalties for failures to release information, increasing the pressure on organizations to make sometimes fast and inaccurate decisions. It doesn't end there – the PHI you are responsible for gets sent everywhere. It starts to look like a tangled web. While you can't be held accountable for the actions of others, the lines can get very blurred and getting dragged into an impermissible disclosure dispute can cost you time and money.

Maintaining that dual posture of securing PHI and making it available where mandated and necessary requires far more than meeting the requirements of HIPAA. Today's cyber-climate is changing at such a rapid pace, no one can or should expect legislation to keep up.



The Gap Between HIPAA Compliance and Cybersecurity

Let's look at the gap between HIPAA and cybersecurity requirements.

1. Firewalls

HIPAA does not provide much insight on firewalls, in fact, it's not even mentioned in the regulation. That means from a HIPAA compliance perspective, even the most basic, rudimentary firewall, hardware or software, could be considered compliant. However, from a cybersecurity perspective, basic solutions aren't going to get the job done. For example, is your firewall configured properly? On too many occasions we've discovered firewalls that were configured so poorly they were just pass-through devices or bridges into the network. Can your firewall do content filtering, antivirus at the perimeter, network segmentation, and provide VPN connectivity? While there's much more your firewall should be able to do, if it can't provide this essential functionality, then you should be in the market for an upgraded solution.

By the way, both at home and in your office, don't assume your internet service provider (ISP) has given you a firewall. It's quite likely you have a modem and not much more. If you're coming into your office from home, either upgrade your firewall or establish a VPN channel for remote connectivity. It only takes one hole in the dike to drain the data, don't be that hole.

2. Network Segmentation

Network segmentation is one of the most effective ways of keeping your data out of the hands of miscreants, and guess what, HIPAA doesn't require it. We're not talking about simple access privileges, we're talking about configuring your network such that critical PHI, for example, is not accessible from users in other areas. One approach is to put your web servers, your database servers, and your users on different, or segmented networks. Not only will this typically improve the performance of your network, but it will help to isolate a compromised segment so a hacker can't get to other sensitive data.

There are several different ways to segment a network. If your network isn't currently configured with segmentation, it's a good idea to look into it. It can be done very inexpensively.

3. Vulnerability and Penetration Testing

Do you know what your technology footprint looks like to the outside world? If you aren't conducting regular penetration testing and/or vulnerability testing, chances are you don't know. Once again, conducting these types of tests isn't required by HIPAA, and they're not included in most Risk Assessments. If the excuse is cost, it shouldn't be. While it's true penetration testing can be pricey, vulnerability testing can be done very cost-effectively. We believe so strongly in this being necessary that we include network vulnerability testing as part of our HIPAA compliance program.

If you aren't conducting these tests on your organization, you need to seriously consider it. Even basic dark web scans can yield insights into your operation that may prove helpful, and some of those are free.

4. Access Log Reviews

Log reviews are also a HIPAA requirement. Specifically, you're supposed to be reviewing access logs and recording them in a ledger when you do it. The reality, however, is manual log reviews are tedious and impractical. If you've never seen the data file from a firewall or network switch, they look like gibberish to most of us. As a result, it's probably the single biggest area where organizations, smaller ones, in particular, fail to meet HIPAA. It's also the reason we hear about breach reports when the initial attack began a few years ago. The victim simply didn't know they'd been attacked because no one was reviewing their access logs (among other incompetency).

So how does one go about meeting this HIPAA requirement in a practically and effectively way? Enter the SIEM – Security Incident and Event Manager. Initially cost-prohibitive, web-based solutions have driven down costs on SIEMs to make them more attainable for most organizations. Get a SIEM through a SOC (Security Operations Center), and you've now got a group of professionals managing your security.

If all of that sounds too expensive, then it's time you reconsider what basic business operational costs are today. Years ago, we all accepted the fact that computers needed virus protection software, and while there were free ones, many of us ponied up to buy highly-regarded products like Norton Antivirus. Much like those days, today's climate is such that we need to invest more in our security than we used to. The sooner you accept this shift in our realities, the sooner you can adjust your business economics to accommodate these new requirements.

5. Backups

Along the same lines as your security infrastructure, if you haven't updated your data backup technology in the past few years, it's time to reconsider. Gone are the days when tapes were stored in locked cabinets. Gone are the days when external hard drives were taken home each night by key personnel. They are gone, right? If you're solely relying on remote, or offsite backups, any idea how long it takes to download your data to restore operations? In many cases, even for smaller organizations, it's days and weeks. Conversely, if you're relying solely on local backups, a break in or disaster could wipe you out.

Meeting today's cybersecurity and business continuity demands dictate a more robust solution, and a BDR, or Business Disaster Recovery device, is the answer. A good BDR will allow for near real-time backups, will take backups offline and make them unavailable to the network to defend against an attack, will co-locate backups in more than one offsite location, will encrypt it all, and can be used as a short-term server should your primary server suffer a meltdown or other attack. Why do we suggest BDR? For one reason, it's the ONLY reliable way to survive a ransomware attack. If you're hit with ransomware, you have 3, and only 3, options. One, pay the ransom – pay and you have no guarantee you'll get your data back, or that you won't get hit again tomorrow or the next day. Two, lose your data and walk away from it. Or three, restore everything from backup. While you may build the Fort Knox of security to protect against an attack, one errant click from a user can blow the safe wide open. Again, having a solid backup strategy is the ONLY way to reliably survive a ransomware attack.

Basic Principles

I believe one of the reasons people consider HIPAA to be so frustrating is because they get caught up in the minutia of meeting all of these requirements. It is possible, however, to break HIPAA compliance down into a few basic concepts that simplify the requirements.

Minimum Necessary Rule

The most basic principle in secure data management is most commonly known as the Minimum Necessary Rule. Our preference, however, is to refer to this as the Minimum Access Principle, or MAP. The premise of the concept is to restrict all access to sensitive data as the default state. Put another way, no one has access to anything. From there, add permissions to those individuals, and to the specific data they require to perform their work functions and nothing more. Approaching this from a default setting of zero access, and building from there is a more secure methodology. The traditional technique of all access is granted by default, and restricting access as needed, leaves room for gaps and errors. From a data manager's perspective, it's better to loosen controls that are too tight than to attempt to tighten controls that are too loose.

Implementing MAP varies by organization. Larger organizations may segment their access based upon defined departments. Smaller organizations tend to create access policies for individual roles. Both methods are equally effective, although the departmental approach may limit the ability to implement tighter controls for individuals within the department. For example, a front office may have a department for patient registration staff. Within that team, there may be individuals who don't require the same level of access as others; interns, students, part-time workers, for example. A department based MAP approach may grant unneeded access to these individuals and that's not preferable. Is it a HIPAA violation? Potentially, but the larger concern should be the increased risk that one of those users may trigger, or be the source of a breach of information they didn't need access to in the first place.

MAP roles change. This is not a set-it-and-forget-it policy. New devices, new users, new services being offered, all represent change where MAP must be addressed. This is another reason we recommend the zero default access state for all new devices and users on your network, and building up access from there.

Basic Principles

Managing ePHI

Once ePHI has been created, it has two states, at rest, and in transit. HIPAA requires ePHI to be encrypted in both states – sitting still on your servers and when it's in motion.

ePHI at Rest

Let's look at idle ePHI and look at two examples. Let's consider ePHI in a database and ePHI in the form of PDF files that may be residing in a folder on your server. Please note that I am isolating the storage of ePHI to your server, and not distributed on workstations across your network. If you have ePHI all over your network, hopefully, you recognize the exponentially increased risks you have and are working towards reducing that exposure. Back to our server. In both cases, whether in a database or folders, the ePHI needs to be encrypted. Encryption can be done within the database, at the file level, at the folder level, or even the entire hard drive that stores all of it. How you choose to encrypt your data is up to you. Different options have different implications, like overall system performance, for example. Again, if you feel yourself getting mired into the details, don't. That's when you call your IT, inhouse or otherwise, and ask them for their recommendations. Let's consider the case where you have ePHI on networked devices, like EKG or imaging machines. You may not have the luxury of pathing their data storage to your server, but instead, you may be stuck with the data residing on the workstation they're attached to, or the device itself. In these cases, it's important to understand what protocols your vendor has implemented for that equipment and act accordingly. To keep things simple, break down your devices into groups, identify which ones store, or could potentially store ePHI, and evaluate how they're being encrypted. If the answer is not at all, and you can't store that data elsewhere, that device goes on your remediation plan for replacement.

ePHI in Transit

When we transmit or move ePHI from our network to another network, like from your hospital to a general surgeon's office, it must be encrypted as it travels. Examples of this would be using an encrypted email system that allows you to send your messages encrypted or uploading a file to a website that has a valid HTTPS certificate. Again, this doesn't have to get complicated. If it's moving, it needs to be encrypted. A simple way to approach this is to identify the channels through which your ePHI travels into and out of your organization. This will include faxing, emails,

file shares, uploading and downloading to and from specific websites. Evaluate how these channels manage that traffic. Is it encrypted at all times? Is it possible for ePHI to be transmitted through that channel without encryption? Identify those channels and processes and plug any weaknesses you may find. It should NEVER be acceptable for your workforce to transmit ePHI from your facility without it being encrypted. If for some reason the ability for this situation to occur exists, then constant training and management are imperative.

External Communications

- If you don't need to include PHI in your communications, don't do it.
- If you need to include PHI, include the minimum necessary.
- If there's an alternative, more secure way to communicate this information, use that method.

These are the types of thoughts your workforce should be considering throughout their workday. In a perfect world, your staff would only be able to convey ePHI securely, but this scenario is rarely the reality. Instead, we live in an environment where sensitive information can be conveyed to the wrong person and conveyed insecurely. Reinforcing the above tenets like a mantra will help keep your workforce thinking as they engage in these tasks.

Passwords

Let's face it. We all hate passwords. We're told we're supposed to have different passwords for everything, that they're supposed to be hard to guess and include funny characters. You know the routine – at least 8 characters long, must include upper and lowercase letters, at least one number, etc. Who remembers these, right? Well, to show you what a great job we all do, the number one and number two passwords in the US for several years running have been the word "password" and the numbers 123456. No kidding, it is that bad! We – all of us – are terrible at passwords. In fact, according to a report by MacAfee, we're so bad that the estimated cost of cyber-attacks on the global economy in 2018 was about $1 trillion. In 2019 that number is estimated to double to $2 trillion. How does this relate to passwords? The truth is the overwhelming majority of successful attacks are caused by compromised user authentication. In other words, stolen or hacked passwords and user credentials are the greatest weakness we face in being cyber secure. So we have only ourselves to blame for creating the fastest-growing, most profitable criminal activity in human history.

But it's not all our fault. We could blame former NIST employee Bill Burr, known as the father of the modern password. He drafted the original NIST specifications for password recommendations and it's his guidance we are still following to this day. Actually, it's not all his fault, either. After all, his recommendations have lasted the past few decades, and given what he knew at that time, and how much things have changed, he did a pretty good job.

Who else can we blame? Well, whoever came up with the term "password", didn't help matters. Our password lives were failed at the premise – the actual name encourages the wrong way for us to be thinking about them. In truth, we need to start using the term passphrase instead. A passphrase is a much more accurate depiction of what we need to be striving for because as it turns out, longer sequences of letters are harder to hack than short words with funny characters.

It looks like the end of our password pain may be on the horizon. To account for the changing threat landscape, and our atrocious behavior with password rules, NIST published updated guidance to follow. Among those recommendations are longer passwords, no more requirement to change passwords frequently, and less emphasis on funny characters, among other things. Here's the premise for the NIST password recommendations. Primarily, the software that's used to hack many systems simply cycles through all keyboard characters at blistering speeds. It doesn't consider if it's a capital letter or an obscure character, it just crunches away until it succeeds. These types of brute force attacks are common, and anyone who has ever looked at firewall access logs has seen them in action. So the great news is, make your passwords easier,

Passwords

but longer. Don't change them regularly, and don't worry about confusing characters. Terrific, right? Not so fast.

We don't fully endorse the new NIST requirements. Here's why. While they are correct as an anecdote against brute force attacks, they don't cover the more common types of attacks – someone guessing your password, still a leading method of attack. In other words, we believe a certain degree of complexity is still beneficial in keeping your password protected.
Let's look at what constitutes a more secure password. First, longer is better than shorter. Here's a quick example of what I mean.

In this example, I'm going to use a simple password, in fact, one of the most common passwords. Here I'm entering the letters p-a-s-s-w-o-r-d and then the numbers 123. According to Kaspersky's online password checker, this password would take a home PC 6 seconds to hack. Now, if we added a couple of more digits, that time increases to 4 days. The point here is obvious and simple. Just adding a single character to your existing passwords is a step in the right direction, but that still doesn't create a good password.

Let's take this even further. Here are some things NOT to do when crafting your passphrases:

1. Don't use popular words or words in the dictionary – password, goofy, football, Go Pittsburg Stealers.
2. Don't string together words that are commonly together – i.e.. My boss is a jerk
3. Don't use your username or email address
4. Don't use sequential characters – 123456, abcbeyonce are terrible passwords

Now let's look at a few tips that will make your passphrases harder to crack but still easy to remember:

1. Mix numbers or special characters into your passphrase. Instead of adding numbers at the end of your password, put the numbers somewhere in the middle. So a password like "My3d0g9Spot!" is much better than "MydogSpot39!"
2. Better yet, create a sentence that is easy for you to remember and long. For example, take: "my dog spot ate his breakfast and then threw up!", and mix it up to look like this: "mD5s8ahb@ttu!". Here we added a number and only used the first letter of each word. It's a strong password, but it's still not going to be the easiest to remember.

Passwords

Password Managers

Modern password security does warrant a more sophisticated solution, and that's where password managers come into play. There are many to choose from, LastPass, KeyPass, Dashlane, Roboform, and more. Most function in a similar manner. You create one, very strong password, and that lets you into the software where all of your passwords are stored. With browser plugins and mobile apps, a good password manager will have your password at the ready wherever you need it. The biggest advantage to a password manager is you can use the random generator they include to create incredibly complex, long passwords that you don't have to remember.

The downside to password managers is they have an Achilles Heel – they rely upon a single password you must remember to gain access to all of them. While that weakness can be diminished with Two Factor Authentication, biometric authentication, and a complex password you memorize, it's a concern none the less. However, for that weakness to be exploited, you must be the target of an attack. More often than not, hackers are targeting much larger honeypots than individuals. They're more interested in attacking Target and Macy's, where they can gain identities on tens of thousands of people at a time than they are Cindy Lou from Whoville. That said, if Cindy Lou works for Target or Macy's, she can be employee zero in a targeted attack, although they'd be after her company network access credentials.

Hope and despair on the horizon

I previously mentioned the use of Two Factor Authentication. In short, 2FA is the addition of a second metric for identity verification. In this case, the password is something you know, and the 2FA authentication is something you have. 2FA is most commonly implemented by sending the user a text message with a code to enter to gain access after their user credentials have been entered. While this is not a bulletproof solution, it's a big step forward and requires considerably more skill for a hacker to bypass.

Passwords

The second evolution we're encountering is the use of biometrics as an authenticator. Facial recognition, fingerprint scans, retinal scans; these are examples of biometric credentials. Again, while those help considerably, they're not foolproof either, and more concerning, if someone gains access to your fingerprint, digitally or otherwise, how do you change that?

For now, the combination of complex passphrases, biometric authentication, and 2FA are the best we can do, and they're miles ahead of just passwords alone.

I mentioned despair is also on the horizon, right? Have you heard of quantum computing? Quantum computing is the equivalent of going from horse and buggy to the Model T in computer terms. Blistering speeds and processing power will usher in another revolution in technology. With that power comes the ability to render all of our present level encryption and authentication measures obsolete. Good thing it's still years away, right? Not quite. China has invested billions into a quantum computing facility they claim will be online in 2020. While we don't exactly how short the window is that we have left, we do know things will be changing with our authentication methods very, very soon.

Faxing

We get more questions regarding secure faxing than any other area of HIPAA. Our first response is always the same – why do you want to use faxing? By now, certainly in healthcare, faxing should have fallen into the same heap as your ditto machine and your pagers. Sadly, that's not the case. Many organizations still rely upon faxing to send and receive critical patient data.

Answer the following question – which of these answers regarding faxing Protected Health Information is correct?

a. It's never HIPAA compliant to send PHI in a fax

b. Faxing is secure, point to point method of sending sensitive information and is, therefore, HIPAA compliant

c. Faxing PHI is HIPAA compliant only if the intended recipient is contacted before the fax is sent and a confirmation of receipt is sent in return.

If you guessed A or B, no soup for you. Sending a fax to an unattended fax machine means anyone walking by could pick it up, and they may not be authorized to view its contents. The only correct answer is C.

Here are some tips to consider when it comes to faxing PHI:

1. Replace traditional fax machines with a HIPAA compliant, secure, electronic faxing service. There are several providers of HIPAA compliant faxing solutions who provide a cost-effective alternative. We've worked with Rightfax, Sfax, and efax over the years. Each offers viable solutions. If you go with an eFax solution, they must sign a Business Associate Agreement. They may argue they are merely conduits, like your phone carrier, but they are not. Your faxes route through and often reside on their servers. That makes them a Business Associate. If they won't sign a BA, move on to another provider.

   On that same note, it's important to confirm your faxes are being encrypted in transit and encrypted at rest. Simply signing a BA, although binding the vendor to adhere to HIPAA, doesn't mean they're doing it. It's best to confirm it in writing.

Faxing

2. Contact your intended recipient before sending the fax, and then confirm their receipt of the fax. This is the only way to ensure accuracy and that the fax doesn't sit unattended on the recipient's device.

3. Use a cover page. The use of a cover page enables you to provide the required HIPAA compliance verbiage. Here's an example of the verbiage EVERY fax you send should include on the cover page:

   The documents accompanying this facsimile transmittal are intended only for the use of the individual or entity to which it is addressed. It may contain information that is privileged, confidential and exempt from disclosure under law. If the reader of this message is not the intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you are not the intended recipient, you are hereby notified that law strictly prohibits any disclosure, copying, distribution or action taken in reliance on the contents of these documents. If you have received this fax in error, please notify the sender immediately to arrange for the return of these documents.

4. Monitor your fax machine(s). At least one staff member should be tasked with monitoring your fax machine(s). Leaving incoming faxes unattended can easily lead to an impermissible disclosure, particularly if your fax machine is in a publicly accessible area (if it is, move it).

5. Be sure to track where your PHI is being stored, and that documentation should include your networked fax machine. These devices retain sent and received faxes, and as a result, they require you to treat them like any other endpoint device with PHI on them. That includes implementing a proper disposition policy when disposing of or replacing the device.

6. Maintain an audit trail of sent and received faxes. Electronic fax systems simplify this requirement, but even your traditional fax maintains a log. If you're using traditional fax, it's recommended you regularly print your fax logs and store them in a designated binder.

You are correct to conclude faxing PHI properly is a challenge and potentially not worth the risks. Converting to an electronic fax solution should be on your shortlist of tasks to complete. Moving away from faxing completely should be your long-term goal. Keep in mind, the content of a fax is dumb data - it can't be easily converted into a database, so the information faxes contain have limited value to your data analysis efforts anyway.

Texting

Your patients want it. You probably want it. It's become such a common method of communicating that many of us rely upon it more than we do talking on the phone. And for good reason. It's fast, efficient, and simple to use. Why, then, so much fuss about using it in a healthcare setting?

For starters, texting (SMS, or Short Message Service) was never intended to become what it is today. Literally, trillions of text messages are sent annually. While the architecture supports the volume, it's not a secure messaging platform, and it was never designed to be one. Complicating matters, newer technologies exist, like Apple's iMessage and others, do away with the SMS architecture and use Internet Protocol-based communications.

The challenge, then, is how do we securely send text messages in healthcare? Over the past few years, some companies have entered the secure texting arena, several of them are focused on the healthcare industry. From free options like OhMD to enterprise-level solutions like TigerText, the range is now broad enough that anyone in healthcare who wants to open up texting as a communication channel can do so.

Most of these products work similarly The user can choose to download a mobile app, use their website, or both. This approach allows messages to be contained within the vendor's secure, encrypted network. In other words, secure texting is not a plugin that you add to your phone's texting app and voila, you're secure. Rather, it's a dedicated application that senders and receivers will all utilize. Since patients can create accounts and use these applications, they're a viable and practical solution for both providers to provider communications and providers to patients.

Emailing

The use of email in healthcare has grown exponentially, as have the threats email poses. In fact, in 2018 email-related breaches rose to 31% of all healthcare breaches, more than triple what it had been in the previous 8 years. It's not surprising then, that phishing schemes and other types of email-based attacks have become so sophisticated and prolific – they're working.

As an industry, we have made a choice. Email is an essential component of our communications and those who don't use it will be considered behind the times with both peers and patients. It is therefore vital that email is implemented and utilized securely. Let's look at what the vulnerabilities are you exposing yourself to and how to use email properly.

First, one of the most frequent questions we get is whether Gmail and Office365 are HIPAA compliant. I know folks are looking for a simple yes or no answer, but that's not accurate. The truth is, the answer is maybe – it depends on both how it's been configured and how it's being used. Out of the box, no, neither solution meets the requirements of HIPAA. Configured properly, following their specs to the letter, and then using those clients as conservatively as possible (sending the minimal information necessary), HIPAA compliance is achievable and maintainable. Of course, many users will implement these applications themselves, or work with IT that is not as familiar with HIPAA as they represent. The result is we often take on clients who are not set up properly, have been that way for years, and end up having to make changes.

But what if the patient has authorized the use of email to send their data? That's a great point. Here again, it's not a "sure, then you're good" answer. When you say they authorized it, how did they do it? Was it over the phone? Was it part of your Notice of Privacy Practices? Was it a separate agreement? Did they authorize the use of email to communicate with them or did the authorization specifically state the use of email to send PHI? These are critical questions to get right, even if your deployed technology is encrypted in transit and at rest and otherwise, HIPAA compliant. In other words, tacit approval isn't enough. Clearly stated and documented authorization is vital.

Why is it so important to seek authorization if we are sending all of our emails in a HIPAA compliant manner? In short, email in the best of scenarios is full of fault lines. Recipients, particularly elderly may share an email address. The elderly may also have family members who access their computers. The potential for PHI to fall into the wrong, or unintended recipient's hands when sent through email is significant. Getting specific authorization improves your position when and if something goes wrong or someone gets upset.

Emailing

While email is an entrenched platform for communications, there is a better way to go. We look at communications as either email-based or portal based. Portal based email or texting requires the recipient to log in to a website or application to open the message and read it's contents. That way if the message is received by the wrong party or family member, that person would have to know the user's access credentials at the portal to view the substance of the message. Both approaches have their advantages and disadvantages. Direct email is faster and doesn't require the user to access a different application to view it. Direct email is also easier to send since it's sent from the email client itself and not email from a portal. The advantage of a portal is you have a considerably more secure solution that only the appropriate recipient can access. Plus, you aren't leaving PHI in the sent box of your email client.

Which approach is better from a cyber-threat perspective? With email being a major target of hackers, the less dependent you are on it, the better. Let's play out a basic scenario. You receive an email from a prospective new patient with an attachment called "mymedicalrecord.pdf". You then receive a call from said patient asking if you received the email and if you've looked at it yet. You promptly open the PDF file only to discover nothing happens. "Oh, can you send it again, it didn't open". The supposed patient says sure, then I'll call you back. But they never do. What just happened was you were phished, and that PDF that "didn't open", did indeed open, and it ran a program opening up your computer to the sender, who also made the call using a spoofed phone number. Once that patient/sender/hacker is into your machine, they use other software to steal your credentials, upgrade themselves to system administrators, and then traverse your network seeing and doing whatever they please.

Let's consider a portal-based approach. In this same scenario, the patient wouldn't be sending you a direct email, they would have to be communicating through your portal. That requires them to have an account, which becomes the first hurdle. Second, instead of an attachment, they would be uploading this document into the portal, where tests can be run on it to make sure there are viruses or malicious code attached. Third, your portal should allow you to view the document before to downloading it into your organization's network. Using the web-based viewer, it would either error out or nothing would show and any code would be blocked at the web-server.

The message here is portal-based communication is exponentially more secure than internal email clients for both providers to provider and patient to provider communications.

Emailing

Phishing and other email threats

Email attacks are the single largest cyber threat your organization faces. These threats primarily come in two broad categories, phishing attacks, and business email compromise (BEC) attacks. We're not going to go into details on these threats since that's more about cybersecurity and less about HIPAA compliance, but understanding the nature of the attacks is an important component to understanding the risks your organization faces when using email for communications.

The majority of email compromises are created by phishing campaigns or emails sent by malicious actors seeking to trick the recipient into clicking a link in the email or opening an attachment. In some cases, simply displaying images in an email can launch an attack. Phishing schemes have been around since the inception of email, but they've evolved into cleverly crafted and targeted attacks that have allowed them to continue being very lucrative for hackers. The goal of most phishing campaigns is to gain access to the enterprise network. In many cases, that includes stealing user access credentials or launching ransomware or other malware attacks. As mentioned previously, once these credentials have been obtained, they use that access to elevate their privileges and traverse the network, gaining access to whatever they want.

BEC attacks have rapidly grown in popularity and profitability for hackers. These types of attacks use social media mining and other tactics to gain information on a targeted organization and its employees. They'll become a "man in the middle" of an email string between the CFO and an accounting staff member, for example. When the time is right, they'll step in and send an email acting as the CFO and convince the staff member to send a pending wire to an altered wire address. This type of attack has cost US businesses billions of dollars in just the past few years alone and shows no signs of slowing down.

Email is an essential part of business operations, and that holds true in healthcare as well. In fact, email use in the healthcare sector is increasing. With this level of reliance and the associated risks, healthcare organizations need to implement the resources necessary to mitigate those vulnerabilities. From a HIPAA compliance perspective, organizations need to implement and utilize email compliantly, but they also must make proper investments to secure themselves to ensure they're not deemed to be "willfully negligent".

Emailing

Use of Mobile Devices for Communicating PHI

Here is something to keep in mind the next time you grab your phone to send a text. If you ever find yourself in a lawsuit against a patient, and you use your phone for a patient or provider communications - ALL of your phone records will be discoverable - ALL of them. That may be a bit unnerving to hear, but it's a reality, and it happens often in legal proceedings. If this is a concern for you, then we encourage you to maintain separate devices for personal and business use or consult with your counsel for guidance on ways you can avoid being forced to disclose communications that may be highly personal.

Social Media in Healthcare

Social Media in Healthcare

The era of social engagement is well underway and it's having a dramatic impact on our society. Healthcare has not been spared by its impact either. Many healthcare organizations have embraced the use of social media to share their message, their achievements, and to promote new services they're offering their communities. Individuals have also utilized social media to share their health experiences and to voice their displeasure with providers or organizations when things haven't gone as they expected. Like it or not, social media is here to stay and it is vital for your organization to understand how to maneuver in this new world. For clarity, when we're discussing social media, we're primarily referring to Facebook, Instagram, LinkedIn, and Yelp, but any social sharing application applies.

We break social media into two separate components. There is social media for your organization and social media for the workforce. We recommend maintaining two separate policies to address this.

Organizational Social Media Engagement

Get the word out – that is often the mandate for a hospital that has invested in new services, a new urgent care facility, or a tech start-up with an innovative care delivery model. One of the more effective mediums for doing that today is through the use of social media. Without question, brand reputation can be enhanced or destroyed on social media alone. Healthcare organizations cannot afford to ignore their presence on these forums but getting organizational social media right has proven to be more difficult, and fraught with pitfalls, then many realize.

Why is social media so risky? For starters, patient photos showing up on social media have been at the heart of numerous HIPAA violations. On several occasions, the acts were intentional, where staff members posted photos of patients along with comments. On other occasions, the postings have been inadvertent – a staff photo of a birthday party accidentally included patient charts with names visible, or patients in the background. Regardless of the cause, OCR frowns upon those types of behaviors, and your organization will see that disappointment expressed by way of fines and penalties.

HIPAA spells out quite specifically how PHI can be used for marketing and promotional purposes. Unless you've followed these requirements, you shouldn't dare tread there. For those organizations that aren't organized and coordinated in their social media activities, the Office for Civil Rights is waiting for you. What do we mean by being coordinated? If your marketing campaign today or tomorrow includes patient information, be it photos of patients, or quotes from patients on brochures, websites, or email campaigns, then that effort needs to be coordinated with your policies and your patient documentation.

Many organizations will embed PHI marketing use language within their Notice of Privacy Practices (NPP), which they will then make available for patients to review in a binder in the waiting room. When it comes to your NPP, while it may be HIPAA compliant to simply make it available to your patients, we strongly encourage you to have your patients sign an acceptance that they've reviewed the information as part of their registration packet, for example. If you intend to use PHI for marketing purposes, you should present such intentions to your patients on a separate form and have them sign that form to become part of your record. Again, while that may not be required per the letter of the HIPAA law, it reduces your risk and will make the attorneys tasked with defending you happy. Your first social media policy should define your intentions for using social media on behalf of the organization. It should state whether or not you will use it, how you will use it, will it include PHI, and specifically what purposes you intend to use it for.

Social Media and the Healthcare Worker

This is one of the subjects that I address when I speak on the subject where I get groans from the audience. Some of my audience members have argued my recommendations may not be legal. They may be right. Let me explain. If you choose to have a career in healthcare, then you take on a responsibility to be a steward of people's most sensitive and personal information. Whether you're a receptionist, a surgeon, or a hospital administrator, you all share that same obligation. Unfortunately, we live in a time where your behavior on social media for your personal life can have a huge and adverse impact on your employer. Through social engineering, hackers and data aggregators collect as much information as they can on individuals with the intention of either compromising them, convincing them to share their credentials, or simply guessing at their access credentials. This method of attack often manifests itself as a component of a phishing attack. Although random phishing attacks still exist, the trend has been towards highly targeted

attacks towards specific organizations and individuals. What this means is everything that your workforce posts on social media, whether it's regarding your organization or not, can and will be weaponized and used against you.

The second social media policy your organization needs to have addresses the use of social media by your workforce. The policy needs to define under what circumstances if at all, your workforce can discuss or post photos of your organization. Do you want your workforce to even access social media while they're on your campus or the premises? These are some of the considerations you need decide upon when creating your workforce social media policy. Ideally, your workforce will refrain from posting on social media at all, but while you can request that, as I mentioned above, it's probably not legal.

Why do we take such an extreme position on social media? If it weren't for the effectiveness of social media-based phishing attacks, we wouldn't care, provided the postings weren't disclosing PHI or crossing other disclosure restrictions. But social engineering, and the use of that information to attack an organization is costing our country hundreds of millions of dollars a year, and over a billion dollars worldwide. Any information your workforce shares publicly is being gathered, organized, and leveraged to attack you. In fact, given the accuracy of facial recognition software, it may not even be wise to continue posting staff photos on your website. We have to accept that we live in a new era where all of our information can be used against us.

The subject of cybersecurity deserves more attention than we can cover in this ebook, but you should be aware of its impact on healthcare organizations and the gap that exists between HIPAA compliance and being cyber secure.

Now that you've got your social media policies set, let's address the use of mobile devices in your organization or BYOD.

Bring Your Own Device Policy

Do you have a BYOD policy? If you don't have one, you need one. Organizations across all industries are increasingly allowing their employees to carry and use their own mobile devices to conduct business, both onsite and off. The implications of what you allow are significant. You also need to use proper documentation. In short, you should have a BYOD agreement that your workforce whom you allow to use their own devices sign, and a BYOD policy that states your position with such devices. For example, if your policy is to allow your staff to use their mobile devices on a guest network in your facility, but not to conduct work-related tasks or communications, your policy should say so. If your policy is to allow staff to use their mobile devices to conduct business, then you need to document that also, and you need to define what controls you're permitted to have. For example, do you require the ability to remotely wipe their device? No? Then what happens if they lose their phone or tablet and that device has PHI stored on it or has access to PHI? What if they leave your organization, do you have the right to remote wipe it then, or are you going to rely on them to remove any PHI or access to your network they may have? Do you have your security controls on their devices, or are you relying upon them to be keeping their antivirus and software up to date?

The security risk of allowing your workforce to use their own devices to conduct business on behalf of your organization is considerable. Allowing them to use their own devices on your network is equally problematic. Limiting BYO devices to a separate network, like a guest network, reduces that risk.

When it comes to BYOD, first decide what you will allow, then document it with both a policy and an agreement between your organization and your staff. This is language that can be included in your Employment Agreement or Confidentiality Agreement.

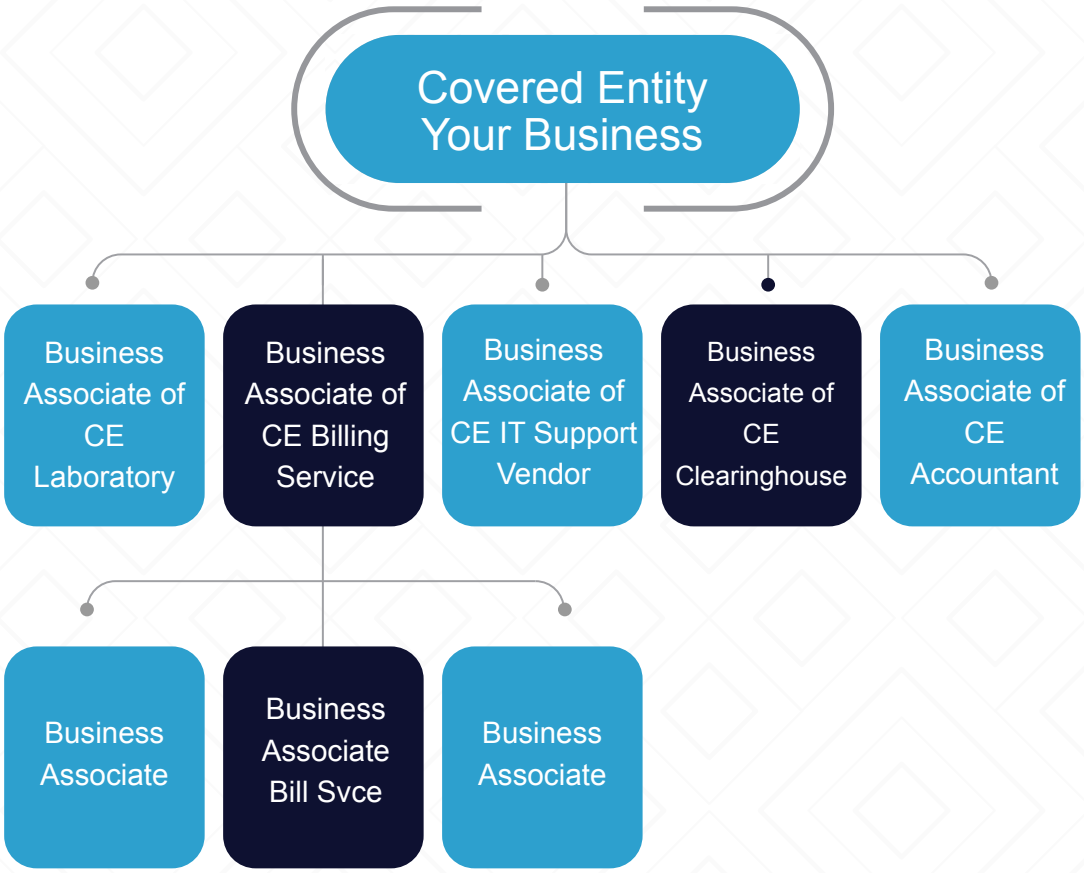
Business Associates and other vendors

Healthcare vendors range in scope from accounting firms and attorneys, to janitors and cleaning services. In between are software vendors, medical device manufacturers, and many, many more. It's been estimated that healthcare vendors are responsible for 20-30% of the breaches that get reported to HHS each year, with some of them being the largest breaches in the industry. Vendor and supply chain management is becoming increasingly critical for Covered Entities. We're going to break down this section into 3 parts - what does having a signed BA accomplish for you, who is a Business Associate, and evaluating your vendors.

What does a signed Business Associates Agreement mean?

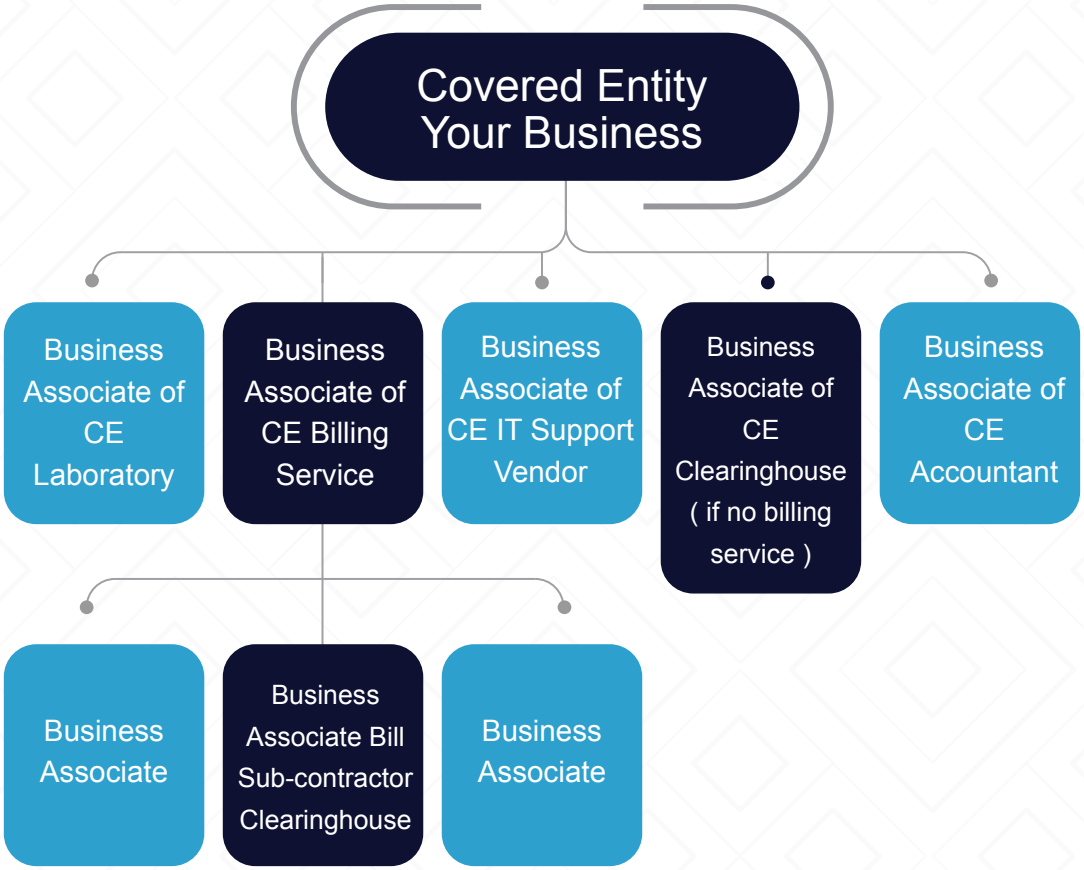
The Business Associate Agreement, properly documented and executed, gives a Covered Entity the potential to distribute risk among their Business Associates. Essentially, if a BA experiences a

Chain of Liability if BA is ab Independent Contractor



Business Associates and other vendors

Chain of Liability if BA is an Agent



breach, the CE is somewhat insulated from the full financial and legal impact of the consequences. Instead, the BA bears the brunt of the incident. Of course, this is true in theory. In the real world, everyone involved in a breach gets put into the line of fire. The public relations hit a CE experience isn't diminished by the fact that their vendor experienced or caused the breach.There is one caveat to the ability of a BAA to shift risk. In the Omnibus Rule of 2013, the legal concept of Agency was introduced into the HIPAA laws. In short, if a vendor is deemed to be an agent of the CE, as opposed to an Independent Contractor, then the risk is retained at the CE level.

Agency is created when one person – the agent - will be a representative of another – the principal. The agent has a fiduciary duty to the principal, which is the highest standard of care imposed by law. The agent must not put their personal interests before their duty. The fiduciary relationship is highlighted by good faith, loyalty, and trust on the part of the agent to the principal.

Business Associates and other vendors

The general rule is that an individual is an independent contractor if the payer has the right to control or direct only the result of the work and not what will be done and how it will be done. As an Independent Contractor, the BA does not have a fiduciary duty to the principal and can earn as much on a transaction as they can induce the borrower to pay.

This graph depicts the risk to the CE if the BA is deemed an agent versus an independent contractor. What constitutes an agency? As mentioned previously, in the law, agency encompasses a broad volume of cases and precedents, so it warrants a conversation with your attorney if you have a question. In simple terms, a court will look to the amount of control you exert over the person you have hired to determine whether or not the person you hired is an independent contractor or agent. An agent is more similar to an employee than an independent contractor. The more you treat a vendor like an employee, the more likely they'll be deemed to be an agent, and that diffuses the effectiveness of using a BAA as a hedge for risk.

Who is a Business Associate?

How do you determine what vendors are Business Associates? If your vendor works with or has access to your PHI in the course of doing their tasks for you, then they fit the definition of a Business Associate. By contrast, if your vendor has only incidental contact with your PHI, like a janitor or landlord, for example, they may not be BA. However, because they may on occasion be able to view PHI, we recommend they sign a confidentiality agreement. If you aren't using a HIPAA compliance service like HIPAA Security Suite, then we suggest creating a spreadsheet of all of your vendors, identifying who is a BA and who is not, and then tracking who has signed your BAA or Confidentiality Agreement and who has not. This will simplify tracking your vendors.

Evaluating your vendors

Healthcare is unique compared to other regulated industries in many ways, not the least of which includes regulations requiring vendors to meet specific guidelines. These guidelines were encapsulated in both the HITECH act of 2009 and the Omnibus Rule in 2013. Healthcare organizations are required to have the vendors they work with who handle or have access to PHI agree to sign Business Associate Agreements. A Business Associate, by signing a BAA, agrees to adhere to many of the same HIPAA compliance requirements as their Covered Entity counterparts. Let that sink in a moment. Everything you're going through to achieve and maintain

Business Associates and other vendors

HIPAA compliance is essentially required of your BA vendors. How many of those vendors follow the requirements they've accepted in the BAA has been cause for concern for both healthcare organizations and the federal government. It turns out these concerns have been valid as many recent HIPAA breaches have involved Business Associates. As a result, vendor vetting has become an integral part of the vendor selection process for many leading healthcare organizations, and it should become part of yours also.

Let's first consider the current state of the CE/BA relationship with most organizations. A department, clinician, or administrator identifies a vendor they wish to use to provide a specific service, like IT management or medical billing, for example. A generic Business Associate Agreement is generated, sent to the vendor, and received back shortly thereafter signed by the vendor. This BAA, along with a copy of their Service Agreement, is then filed away, and the HIPAA compliance box is checked. If this sounds like your process, it's time to revamp your approach. This process is barely worth the effort and the BAA isn't worth the paper it's written on. Why? In short, few vendors understand what they're obligating themselves to, leaving you only marginally better off than no agreement at all. If you want to test this out, simply ask your vendor for a copy of their last risk assessment. Often, you'll be met with an awkward silence. Now what?

A proper vendor management policy includes a more thorough evaluation of the vendor's practices before engaging them. In fact, in many respects, an effective vendor evaluation mirrors a security risk assessment. If that sounds like a high bar to set for your vendors and for your staff to achieve, it is, and it should be. Reducing vendor risk is your responsibility and competent vendors who are doing business in healthcare understand your concerns and are cooperative with your process. If you experience vendor push-back, that may be your first sign they're not a good fit for your organization.

Impermissible Use or Disclosures

All of us are susceptible to one of the most common and frequently penalized HIPAA violations - impermissible disclosure of Protected Health Information (PHI). Why is it so common? In short, you're constantly being asked or required to share PHI. In some cases, the person asking, be it a parent or a spouse, for example, are not authorized, recipients. In other cases, your method of sharing isn't HIPAA compliant. Another reason for the high incidence of violations for impermissible disclosures is organizations are required by law to share their PHI with patients. In fact, OCR has begun enforcing penalties for failure to do so. That action will likely serve to create more improper disclosures since staff members will feel a sense of urgency to be responsive and avoid being fined.

Getting this aspect of PHI management and control correct is one of the more important components of your compliance program, and it’s also one of the more challenging. Any workforce member with access to PHI can inadvertently disclose that PHI inappropriately. Not only is implementing proper procedures difficult but keeping your workforce on task over time is equally important. In actuality, follow up assessments for our clients have shown this to be one of the primary areas where organizations fail after setting the correct course. Minimizing this risk requires secure workflow processes and policies, replete with checks and balances, and repetitive workforce training.

Let’s take a specific example to demonstrate how challenging adhering to this can be. Here's a question we often get - if my patient initiates a conversation via text and shares PHI, does it mean it's OK for me to reply in kind? What do you think?
The answer is no. In the best case, replying could be a HIPAA violation that the patient is OK with. In a worst-case, you could have fallen into a trap set by the patient. With the advent of civil penalties for HIPAA violations against providers increasing, you have to be on the alert.

So how do you handle the sharing of PHI? Set it in stone in your organization that requests for PHI must be in writing. Have a form at the ready for the patient to sign designating their authorization. It's not enough just to put it in your Notice of Privacy Practices form, we recommend a specific agreement. If it's not the patient asking, then a procedure must be in place to notify the patient of the request, whenever possible. While this is a "pain" in the real world, it should be the required procedure for your organization. Additionally, all of these releases should be logged into a ledger that includes the requestor’s information, the patient involved, the date of the request, the date of fulfillment, the reason for the request (if appropriate), what exactly was

requested and released, and confirming supporting authorization had been obtained. Again, it's because this is so tedious that so many organizations fail to adhere to proper procedures. As a result, impermissible disclosures will continue to be a leading cause of HIPAA violations.

Impermissible Use or Disclosures

All of us are susceptible to one of the most common and frequently penalized HIPAA violations - impermissible disclosure of Protected Health Information (PHI). Why is it so common? In short, you're constantly being asked or required to share PHI. In some cases, the person asking, be it a parent or a spouse, for example, are not authorized, recipients. In other cases, your method of sharing isn't HIPAA compliant. Another reason for the high incidence of violations for impermissible disclosures is organizations are required by law to share their PHI with patients. In fact, OCR has begun enforcing penalties for failure to do so. That action will likely serve to create more improper disclosures since staff members will feel a sense of urgency to be responsive and avoid being fined.

Getting this aspect of PHI management and control correct is one of the more important components of your compliance program, and it's also one of the more challenging. Any workforce member with access to PHI can inadvertently disclose that PHI inappropriately. Not only is implementing proper procedures difficult but keeping your workforce on task over time is equally important. In actuality, follow up assessments for our clients have shown this to be one of the primary areas where organizations fail after setting the correct course. Minimizing this risk requires secure workflow processes and policies, replete with checks and balances, and repetitive workforce training.

Let's take a specific example to demonstrate how challenging adhering to this can be. Here's a question we often get - if my patient initiates a conversation via text and shares PHI, does it mean it's OK for me to reply in kind? What do you think?

The answer is no. In the best case, replying could be a HIPAA violation that the patient is OK with. In a worst-case, you could have fallen into a trap set by the patient. With the advent of civil penalties for HIPAA violations against providers increasing, you have to be on the alert.

Impermissible Use or Disclosures

So how do you handle the sharing of PHI? Set it in stone in your organization that requests for PHI must be in writing. Have a form at the ready for the patient to sign designating their authorization. It's not enough just to put it in your Notice of Privacy Practices form, we recommend a specific agreement. If it's not the patient asking, then a procedure must be in place to notify the patient of the request, whenever possible. While this is a "pain" in the real world, it should be the required procedure for your organization. Additionally, all of these releases should be logged into a ledger that includes the requestor's information, the patient involved, the date of the request, the date of fulfillment, the reason for the request (if appropriate), what exactly was requested and released, and confirming supporting authorization had been obtained. Again, it's because this is so tedious that so many organizations fail to adhere to proper procedures. As a result, impermissible disclosures will continue to be a leading cause of HIPAA violations.

Breach Response

Breaches can have many characteristics. Impermissible disclosures by workforce members, hacking incidents, and theft are among the most frequent causes of breaches. A breach can involve a single record or millions of records. Identifying that a breach has occurred isn't always an easy task, either. In the case of a hacked network, the organization may not even realize something has occurred. Let's look at such a scenario.

A workforce member receives an email with an attachment that they believe was sent to them from a co-worker. The user opens the attachment, only to find that a blank PDF page opens. Confused, they think nothing of it and move on with their day. The user unwittingly triggered a malware attack. While they've moved on to other tasks, the malware begins the process of downloading more malicious code, allowing the attacker to gain full access to the network, the server, and any sensitive information that may exist. We are increasingly seeing hackers gaining access to networks, and lying in wait for weeks or months before launching an attack. During that time they're surveilling the network, collecting additional user credentials, identifying where and what information is being stored, and more. The frightening reality of this scenario is the federal government believes there may exist thousands of compromised networks that are lying in wait for an attack, and we wouldn't know it.

In a similar scenario, the hacker may exfiltrate a copy of the patient records database, remove any trace of their presence, and disappear into the night with the goods. Often these breaches are discovered when the database gets posted for sale on the Dark Web, or patient information begins surfacing on the Dark Web, and analysts trace it back to the breached organization.

So the problem with breaches is multi-faceted, and so are the steps required once one has occurred. Let's walk through an effective breach response.

Knowing you've been breached

First, you have to know you've been breached, and as we described previously, that can be more complicated than it may seem. Detecting attacks like the ones described above takes technology and diligence. For example, HIPAA requires organizations to conduct access log file reviews, and as we discussed earlier, without implementing proper technology, this activity simply doesn't get done. The result is networks and user accounts may remain compromised for weeks or months.

Breach Response

Why don't more people use solutions like Security Incident and Event Managers (SIEMs) – until recently it's because these solutions are costly and require a level of expertise to implement and manage properly. Fortunately, SIEMs have become more attainable for even smaller organizations, and that will help those organizations maintain greater security and their HIPAA compliance.

Once you know you've been breached, that point in time becomes known as the "date of discovery". That becomes the starting point for a series of what should be scripted events, as detailed in your emergency response policy or your breach response policy, which of course you have, right?

Stopping and Analyzing the Incident

The priority once a breach has been identified is damage control. In the event of a contained incident, an impermissible disclosure resulting from a mistaken release to an unauthorized individual, for example, that can be a straight forward matter. In the event of a hack caused breach, it can be more complex. Different strategies exist for the technical approaches required, but at the heart of all of them is preventing further exfiltration of data, identifying and locking down compromised user accounts and devices, and determining the full extent of the incident. At the same time, the CE's Information Privacy Officer (IPO) should be notified and involved. If the breach is technical in nature, then getting the Information Security Officer (ISO) involved is also necessary. If corrective action is taken within 30 days of the incident's date of discovery, then it's possible for the CE to avoid penalties. Documenting this process is best accomplished using what we call an Incident Risk Assessment (IRA). An Incident Risk Assessment should include:

(1) the nature and extent of the PHI involved;

(2) the unauthorized person who used the PHI or to whom the PHI was disclosed;

(3) whether the PHI was acquired or viewed; and

(4) the extent to which the risk to the PHI has been mitigated.

The IRA is only required if the CE, based on the facts, wants to demonstrate that no notification is required.

Breach Response

While it's true that conducting an IRA is not required in all breach cases, we recommend performing one regardless since the findings can be illuminating and the exercise can be improved through practice. In other words, if there was an obvious breach of more than 500 records, indulging in the IRA may be a moot point since the findings are already known.

Once the IRA is completed and you know the genesis of the breach, you have to then determine what's required according to HIPAA's Breach Notification Rule. The HIPAA BNR requires organizations to notify patients when their PHI has been impermissibly disclosed or breached. The CE can determine the most appropriate means of conveyance, but our recommendation is to send notifications in writing.

If the IRA indicates a low likelihood that PHI was exposed or a "low probability of compromise", then the CE is not required to report the incident to the potentially impacted patients or Health and Human Services.

"… breach notification is necessary for all situations except those in which the CE demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment ..." **Section 160.402**

Notifications and Sanctions

When the damage is contained and information about the incident is collected, it's time to determine if workforce member sanctions are appropriate and who needs to be notified of a breach.

Sanctions resulting from an impermissible disclosure are left to the decision of the CE with this caveat. If your policies call for workforce member sanctions to be applied and they aren't enforced, the CE could be subject to penalties for failure to enforce their policies. So while HIPAA doesn't delve deeply into the internal expectations of a covered organization, it does require a CE to honor and adhere to their documented policies.

In contrast to the specific requirements of sanctions in the HIPAA language, the notification requirement is very well established. Notifications may include HHS, to media, and to the impacted patients themselves. Here are the criteria for notifications.

Breach Response

If the breach involves more than 500 records

For breaches where more than 500 records were exposed, the CE is required to report the incident to HHS within 60 days of discovery.

The CE must also report the incident to impacted patients. In general, the notice must be sent by first- class mail and contain the following information: a brief description of the breach, including the dates of the breach and its discovery; a description of the types of unsecured PHI involved; steps the individual should take to protect themselves from resulting harm; a description of the CE's actions to investigate, mitigate and protect against future violations; and the procedures the individual may take to contact the CE for more information.

Additionally, the CE is required to report the incident to at least one local media outlet, and the information provided must be similar to what is required to send to patients.

If the breach involves less than 500 records

For breaches where less than 500 records were involved, the CE has the option to report the incident at the time of discovery or within 60 days following the end of the calendar year. Although the CE is permitted to submit multiple incidents at year-end, each incident needs to be reported separately.

Reporting can be done to the Secretary of HHS here: Submit a Notice for a Breach Affecting Fewer than 500 Individuals

Regarding reporting the incident to the impacted patients, HIPAA requires the CE to notify all patients whose PHI was compromised. If you find yourself in this situation, it's recommended you offer to cover the cost of identity protection for a reasonable period; a year is common.

If the breach of PHI did not exceed 500 records, then the CE is not required to report the incident to the media.

Concluding Remarks

We tend to lose sight that HIPAA is intended to assist us in protecting health information. If we're successful at protecting it, then it will be easier to share it and use that information to gain insights on our health individually and as a society. The benefits that can be gained from aggregating all of our health information and studying it can be revolutionary. If we fail to protect it, society will not support that effort. Sadly, at least so far, we have failed to demonstrate we're capable of responsibly protecting our most sensitive information.

For many, HIPAA is the equivalent of a four-letter word, but one that brings nightmares, sleepless nights, and anxiety along with it. It doesn't have to be that way. Much of this belief is rooted in the uncertainty and overwhelming nature of the HIPAA laws. It doesn't help that HIPAA compliance, when attempted internally, requires a degree of expertise across multiple disciplines. It could be argued it's comparable to doing your own corporation's taxes. Can you do it yourself? Sure. Will it be correct? Possibly. Will it become a full-time job for an indefinite period? Probably. That's why for so many organizations, outsourcing HIPAA compliance is both practical and cost-effective.

Whether you choose to go it alone or work with a professional compliance company is up to you. Either way, we hope you do your part to protect the information your patients have entrusted you with and that you recognize achieving HIPAA compliance requires an ongoing effort from your entire organization, from the CEO to the receptionist.

Contact us Today

Want to Speak with an Expert?

Need help with HIPAA compliance for your business?

Contact us Today

1 (949) 474-7774

https://www.acentec.com/

info@acentec.com

Contact an Expert Now: https://www.acentec.com/contact/