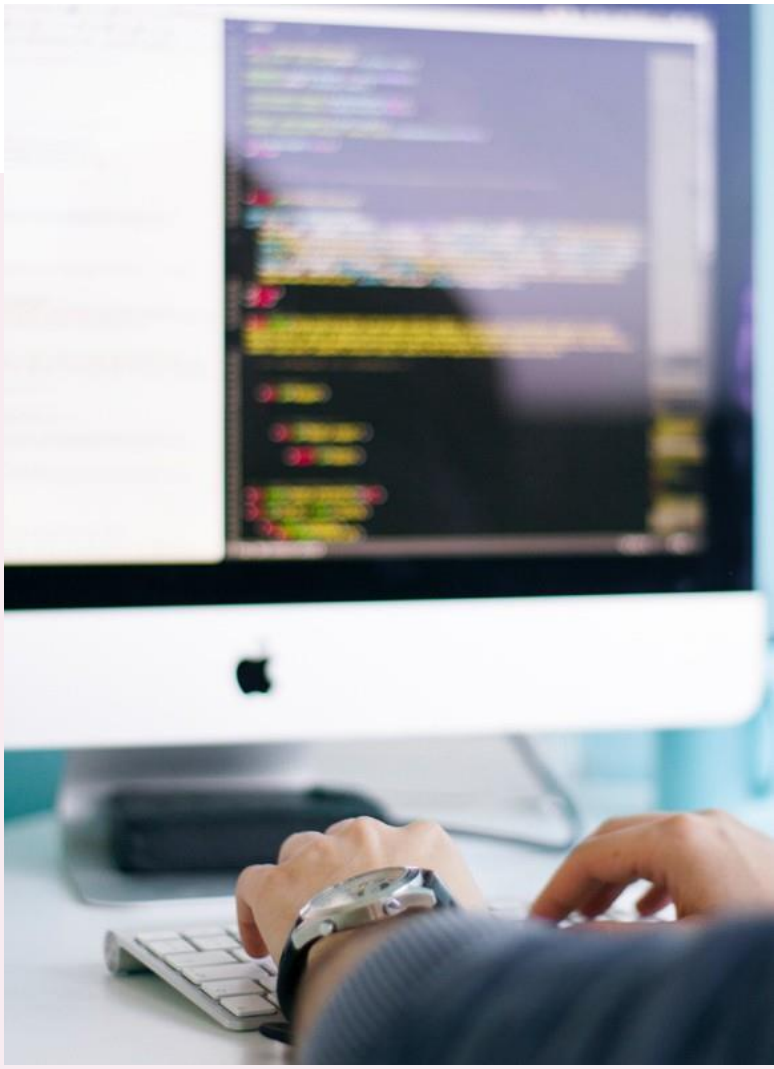
CentraVance

An Introduction to

Cyber Security & Compliance in the Healthcare Fields

By
EJ Phillips

Contents



INTRODUCTION

Security Does Not Equal Compliance

Introduction

In the past 30 years, the medical and dental worlds have changed drastically. In fact, technological advances have changed all industries. These advances, while being both life and time saving, have brought with them more rules and regulations that businesses must follow. Additionally, as we have moved into this age of technology, all data is housed on computers and devices. And just like the homes we live in; businesses can be broken into. But unlike that cat burglar who breaks into your house, the hacker is sitting in the comfort of his or her home, probably in their jammies, hacking into your system. And it is no longer about stealing and pawning, it's about hacking data and selling it to the highest bidder or holding it for ransom. Or both. Therefore, we find ourselves in an era where businesses, and not just those within the healthcare field, must not only secure themselves from outside hacks, they must also comply with government mandates that are ever changing and industry specific. And thus, the marriage between security and compliance was born. And in any successful marriage, both parties must play a role.

Make no mistake secure does not equal compliant. Security can never be assumed to equal compliance, but compliance could very well equal security. There is no one size fits all equation that will meet every business's needs. In order to protect your clients, your patients, your brand, your reputation, your business, you need to make sure that you have both: security AND compliance. And oftentimes, to do this wisely and well, your business will need the help of both IT and Compliance Specialists.

Oftentimes, businesses are excellent at understanding that they need to hire outside IT in order to put into place the best practices for IT and have an efficient working computer infrastructure. What many businesses fail to do is ensure that they are equally strong on the compliance front. You could have the best IT on the planet and still miss the mark on meeting the specific safety standards for your industry. And a failure in either component could be a death knell for your reputation and business. When a business meets compliance standards within its internal security measures, data remains safe and a company's integrity and reputation remain intact. Trust is easy to break, but nearly impossible to rebuild.

Security is all about exercising due diligence to protect the confidentiality and integrity of critical business assets. It is about confidentiality, integrity, and availability. An effective information security program ascertains an organization's security needs, and employs the proper physical, technical, and administrative controls to meet those needs. Security best practices include not only putting in stopgaps to prevent attacks that would harm a business, but also seek to mitigate the amount of damage done when (not if) an attack is successful. Security strategies are ever evolving as today's threats use sophisticated strategies that easily overcome earlier generation technical controls like firewalls, filters, and network segmentation. The modern information security protocol must be proactive rather than reactive in its approach.

Compliance is similar to security in that it also compels a business to practice due diligence in protection of its digital assets, however, the determinant behind compliance is different: compliance is focused upon the requirements of a third party, such as a government, security framework, or a client's contractual terms. Regulations like HIPAA or standards like ISO:27001, outline excruciatingly specific security criteria that a business must meet to be deemed compliant.

Compliance is often seen as that one bossy cousin who comes to Thanksgiving with all the dietary restrictions. But the truth is, unlike your bossy cousin Karen that really is NOT gluten intolerant, being compliant is an asset to a business. Being compliant within a respected industry standard can buttress a business's reputation and earn them new business with security-minded customers. Additionally, a compliance audit will pinpoint gaps in an organization's existing security program that would otherwise have gone unnoticed.

"Being compliant within a respected industry standard can buttress a business's reputation and earn them new business with security-minded customers."

Compliance seeks to go beyond protecting information assets. Compliance oversees policies, regulations, and laws and covers your business from financial, legal, and other types of risks. These are not the primary focus of IT specialists. Therefore, it is imperative to keeping your business's reputation secure that you enlist the help of a compliance specialist. After all, you cannot have a successful marriage with only one party participating. For your business to thrive, you must employ best practices in both security and industry specific compliance arenas.

The team at CentraVance consulting are seasoned compliance specialists with experience in HIPAA, OSHA, SDS, and Cyber Security. To safeguard your business's reputation and your client relationships, contact their team today for a free reputation risk assessment to begin the process of making sure your business is both secure AND compliant.

CHAPTER ONE

5 Steps Towards HIPAA Compliance

CHAPTER ONE

5 Steps Towards HIPAA Compliance

Let's be honest: trying to figure out how to make sure your healthcare practice maintains HIPAA compliance is about as simple and stress free as putting together Swedish furniture while riding a unicycle on a first date. You think, oh there are only these 3 rules I must follow, what could be the big deal? Well, Karen, the big deal is these 3 rules (the HIPAA privacy, security, and breach notification rules) each have subparts, standards, and safeguards. And within these subparts, standards, and safeguards there are various implementations, definitions, procedures, processes, agreements, and controls. Add to that the fact that failure to comply with HIPAA regulations can result in massive fines, civil action lawsuits, and/or criminal charges being filed, should a breach of Patient Health Information occur. Now, unicycling with Sven while building that coffee table is looking like the perfect Sunday afternoon.

So where do you even begin? Just like Sven wants to make sure you have the right allen wrench and all the parts of the coffee table, let's start defining the terms you need to know.

Covered Entity: A covered entity is a health care provider, a health plan or a health care clearing house who, in its normal activities creates, maintains or transmits ePHI using the electronic data interchange.

Business Associate: A business associate is a person or business that provides a service to – or performs a certain function or activity for – a covered entity when that involves having access to PHI maintained by the covered entity. Examples of Business Associates include lawyers, lab techs, accountants, IT contractors, billing companies, cloud storage services, etc.

Angela Simmons, a Certified HIPAA Professional and Certified Cybersecurity expert from CentraVance Consulting, suggests the following 5 Steps towards HIPAA compliance.

5 Steps towards HIPAA Compliance

Step One: Risk Assessment and Analysis

HIPAA rules require that covered entities and their business associates evaluate their ePHI, and all associated risks and vulnerabilities. This is different than a meaningful use risk assessment which only looks at the Electronic Health Records (EHR). HIPAA requires that an entity evaluate ALL ePHI coming in, going out, being created, stored, or maintained by or for the entity. A risk assessment is not a one-time requirement, but a regular task necessary to ensure continued compliance.

Step Two: Risk Management

Once risk assessment is completed, an entity must evaluate threats and vulnerabilities to determine what measures need to be implemented to ensure the security of ePHI. Entities must evaluate and MANAGE risk. Are there reasonable and appropriate controls or measures that can be implemented to help protect the confidentiality, integrity and availability of the ePHI owned or held by the practice?

Step Three: Training

No compliance program is ever complete without training. The greatest risk to an organization will always be the human factor. ALL staff need to be trained on the tenets of the HIPAA rules. This should occur on initial hire and at least annually. The "human element" can be a big problem, and quite honestly, may always remain a large problem in the healthcare industry. Most often employees are trying their best—but if they're not properly trained, they won't know any better and might open a phishing email or click on a malicious link. Training your employees properly and frequently will pay dividends when your employees stop an attacker or malware dead in their tracks.

Step Four: Policy and Procedure

Often entities have many of the tenets of the HIPAA rules in place but have no supporting documentation. The rules require documentation. We should treat HIPAA like we do medical or dental records: if it's not in writing in didn't happen. Your Compliance Plan should include Policies and Procedures ensuring the Privacy and Security of Protected Health Information and the Security of such information. Policies and Procedures need to be updated regularly and any changes need to be clearly documented and communicated to your staff. *The "I didn't know" defense is truly no defense at all.*

"We should treat HIPAA like we do medical or dental records: if it's not in writing in didn't happen."

Step Five: Forms and Contracts

HIPAA rules allow us to use patient information for treatment, payment and healthcare operations without authorization. In order to share information outside of those three parameters, we need authorization. Authorization must be HIPAA compliant, which means it must contain certain elements as outlined in the HIPAA rules. Other forms and contracts might be medical release records, restriction forms, amendment request forms, and accounting of disclosure forms. Perhaps the most important form though is the Notice of Privacy Practices and its companion form the Acknowledgement of Receipt of Notice of Privacy Practices. These notices must not only be readily available to any person who asks for it, but a covered entity must prominently post and make available its notices on any web site it maintains that provides information about its customer services or benefits.

These five steps are not exhaustive to everything a covered entity must do in order to be HIPAA compliant. Like that furniture building date with Sven, there are a lot of moving parts and much is at stake. So get off the unicycle. Call Angela at CentraVance Consulting today for a free reputation risk assessment and to help make sure your healthcare practice is on the right path!

CHAPTER TWO

5 Steps Towards OSHA Compliance

CHAPTER TWO

5 Steps Towards OSHA Compliance

5 Steps for OSHA Compliance

Let's face it: for the healthcare worker in a medical or dental office, the risk of exposure to injury and blood borne pathogens is great. There are literally handpieces, scalpels, and needles used daily. Performing minor surgical procedures, examining wounds, cutting into teeth, or even removing teeth are actual common occurrences! These things are the stuff of nightmares and horror films for the average person, but for the healthcare worker this is simply routine. So how does a medical or dental practice go about ensuring the protection of its workers? Enter OSHA.

According to OSHA.com, the goal of the Occupational Safety and Health Act of 1970 (OSHA) is "to ensure safe and healthful working conditions for working men and women by setting and enforcing standards and by providing training, outreach, education and assistance."

We all want safe work environments. And depending upon what context you find yourself working in, safety can mean different things. OSHA regulations are very industry specific. The Bloodborne Pathogens Standard addresses healthcare workers specifically and is designed to protect at-risk employees from exposure to blood and other potentially infectious materials. Employees and healthcare workers covered by this standard include those who have direct patient/resident contact, draw blood, work with blood and other bodily fluid specimens, and/or handle contaminated equipment. We chatted with Angela Simmons, an active member of the Healthcare Compliance Association, about what steps medical and dental practices can take to ensure OSHA compliance. She gave us the following 5 Steps to take towards OSHA compliance.

5 Steps for OSHA Compliance

Step One: A written Exposure Control Plan

OSHA requires that medical and dental practices have a written plan to address the potential likelihood that an employee is exposed to blood borne pathogens while working with patients. The plan must be specific to the practice and indicate the process for ensuring that bloodwork for the source patient and exposed employee is obtained. Additionally, the exposed employee must receive a free and confidential medical evaluation (this will generally be a medical doctor at an independent location from the practice).

Step Two: Training

The Bloodborne Pathogen Standard requires that exposed employees are trained within 10 days of hire and, at least, annually. Because OSHA is about worker safety, this requirement serves as a reminder that there are controls in place to keep the healthcare worker safe and to reduce the likelihood of their exposure to blood borne pathogens through accident or injury.

Step Three: Immunization

The best defense against disease is immunization. OSHA requires that employers OFFER the Hepatitis B Vaccine (HBV) series to all anticipated exposed employees within 10 days of hire. The employee can show proof, accept the series, or decline the series. The employer must document their effort to provide the series. Employers cannot require titers before they will provide the HBV series to an exposed employee. Since the implementation of the HBV series under OSHA the rate of infection among healthcare workers has declined by 98%.

"Since the implementation of the HBV series under OSHA the rate of infection among healthcare workers has declined by 98%."

Step Four: Engineering Controls

Engineering controls are devices that are designed to isolate or remove hazards, thereby protecting the healthcare worker against exposure to blood borne pathogens. Sharps containers are excellent examples of engineering controls. Sharps containers are designed to be leak proof, spill proof, and puncture resistant. They should be placed at the point of use to eliminate the transportation of dirty, disposable sharps to reduce the likelihood of injury. Another important control is the use of safety engineered sharps that are designed to help protect the end user from injury with the use of guards, sliding sheaths or retractable systems.

Step Five: Personal Protective Equipment (PPE)

OSHA requires that employers provide appropriate PPE to employees. Personal Protective Equipment helps protect employees from exposure to blood and other bodily fluids when working with patients. Employers must provide the appropriate PPE, ensure employees are trained in how to use their PPE, and ensure that employees wear their PPE appropriately based on the tasks they are performing. Examples of appropriate PPE within a medical or dental environment includes, but is not limited to, glasses, gloves, masks, and jackets.

The implementation of these 5 Steps should help your medical or dental practice to be on its way towards OSHA compliance.

CHAPTER THREE

What Does Compliance Training Look Like?

CHAPTER THREE

What Does Compliance Training Look Like?

It's test day. You are sitting in class. (No this is not a dream; you are wearing clothes. Simmer down.) You pull out your blue book and your mind goes blank. You didn't study. You may be dressed, but you will still fail. Compliance training is like studying. No one wants to do it. There are a million other things to do and places to be. But you'll be glad you did it when you are tested.

Training should not be thought of as merely a box to be checked off for compliance. It is best to think of compliance training as an investment in protecting your clients, protecting your business reputation, and empowering your employees. An effective training protocol is one that not only addresses the information your employees need to know, but is tailor made for your business so that your employees digest the material in such a way that they are able to implement the lessons learned. This tailor-made approach to training also ensures that your staff can acknowledge the areas in which they are already excelling and identify their areas for growth.

So what should compliance training encompass?

At a minimum, compliance training should include:

•Identification of the rules, regulations, industry requirements, and areas of risk specific to the training required,

•A qualified teacher/trainer – someone whose specialty or area of expertise is the based in the area of rule, regulation, or risk identified,

•Training that includes all relevant employees (which usually is ALL OF THEM), and

•A record of the training that includes the objectives, summary, and qualifications of the trainer.

CentraVance offers initial training for new employees and annual training for staff to help ensure you meet the tenets of compliance rules. CentraVance's team of experts can provide training in a face to face environment, as a live webinar from wherever you have computer access, or as a recorded training for access 24/7.

CentraVance has training protocols that meet most small business, medical, and dental compliance needs. CentraVance has trainings available in OSHA, Infection Control, Hazard Communication, HIPAA, and Information and Cyber Security Management.

OSHA training for the medical or dental practice should cover the tenets of the Bloodborne Pathogen Standard. This training helps entities understand their requirements to employee safety. This training is required within 10 days of hire for all new potentially exposed employees and, at least, annually.

Effective OSHA compliance training includes:

•Definitions of blood borne pathogens,

•Recognition of OSHA standards related to blood borne pathogens, workers who are at risk of exposure to blood borne pathogens, identification of key aspects of a Blood borne Pathogen Exposure Control Plan,

•Identification of appropriate personal protective equipment (PPE) based on performed tasks,

•A list of work practice and engineering controls in use by the practice,

•A description of the steps to take when exposed to blood borne pathogens,

•Identification of emergency plans of the practice, and

•Identification of employer responsibilities related to compliance with OSHA standard.

"CentraVance has trainings available in OSHA, Infection Control, Hazard Communication, HIPAA, and Information and Cyber Security Management."

Infection Control is about protecting both the patient and the employee. This training is an in-depth exploration of not just the tenets of Infection Control, but what medical and dental practices can do to help minimize the risk of exposure for their employees and the community at large. Ensuring employees are trained in the tenets of infection control helps reduce the likelihood of bad outcomes that can increase risk exposure for any practice.

Infection Control training should include:

•A description of the chain of infection as it applies to infection prevention and control,

•Explanation of methods to prevent the spread of infection,

•A summary of the engineering, work practice and environmental controls that protect against healthcare-associated infections,

•Identification of barriers and PPE for protection from exposure to potentially infectious material,

•Discussion of efforts designed to minimize the risk of occupational exposures to infectious diseases,

•Understanding of sterilization and disinfection protocols, and

•Recognition of CDC guidelines for single and multiple use.

OSHA and Infection Control training is generally for clinical employees only, but sometimes those lines get blurred. It is a good idea for the front desk to have an idea of the tenets of infection control to help prevent patients who should delay treatment based on “X” infection from being seen, unless that condition is the purpose of the visit. For example, if a patient has fever blisters, he or she should not be seen for treatment in a dental practice. If the front desk understands that, they can help protect the clinical employees from confrontation and avoid upset patients.

Hazard Communication is another OSHA rule. It requires that employees are trained about the hazards they face in working with the various chemicals they encounter during their workday. 2013 saw a change to the Hazard Communication Standard, in which Global Harmonization became the new rule.

Under that new legislation, all medical and dental practices were required to train all employees on the new changes to the Standard.

HIPAA training covers the major tenets of the Privacy and Security rule, and how both the employer and employee's play in a role in protecting patient information.

HIPAA compliance training is required for anyone who handles personal health information (PHI). This includes doctors, dentists, hygienists, front desk personnel, etc. Anyone and everyone within a practice or organization is required to complete compliance training, regardless of the organization’s size. Both the large healthcare conglomerate and the country doctor with a pig for an admin must complete the training. Yes, even Wilber the pig needs training. He may be “some pig” but if he handles personal health information, he must be “some trained pig”.

The objectives of effective HIPAA compliance training should include:

•A list of the components of the HIPAA Privacy Rule,

•A list who and what is covered by the Privacy Rule,

•A description of covered entities’ responsibilities under HIPAA,

•A description of how Individuals’ Rights are protected under HIPAA,

•A description of the rules about using and disclosing PHI,

•Discussion of the Security Rule and good security practices,

•Coverage of breach notification requirements, and

•Recognition of the HIPAA penalty and enforcement provisions.

Information and Cyber Security Management training applies to ANY business. All industries gather data. Because of this, we must be aware of the risks to that data. We are no longer in the era of Bonnie and Clyde where bank robberies are in person and pose real risk to human life. Today, bank robberies, and other data siphoning crimes occur from the comfort of the bad actor's home, someone's basement, or in a warehouse, and the bad actor can be anywhere in the world. Understanding the importance of what we protect and how are two very key pieces to this training. This training is for EVERYONE!

Information and Cyber Security Management training should include:

•A demonstration of basic knowledge of cyber security, identify and implement best practices to protect privacy and safeguard Controlled Unclassified Information (CUI) and other sensitive data,

•Recognition of cyber threats to information systems,

•Identification of methods of mitigating insider threats to information systems,

•Discussion of methods of mitigating outsider threats to information systems,

•Identify and report potential cyber security and privacy incidents to the appropriate authority within the organization.

Thankfully, the team at CentraVance knows how to make this training bearable. This training can occur on site at your office, a library, or even a restaurant where you want to feed your staff. It truly doesn't matter. We will train you where you are, at whatever time best suits your needs. Furthermore, the team at CentraVance knows how to make sometimes dry subject matter bearable.

With more than 22 years of healthcare experience, CentraVance principal consultant, Angela Simmons is a Certified HIPAA Professional (CHPC) and a Certified Cyber Security Architect (CCSA). Angela's clinical, managerial and teaching experience make her a great choice to provide employee safety and patient privacy training for CentraVance clients. Her experience in both the clinical and educational settings provides her the insight and ability to identify safety and privacy issues that can occur in both medical and dental offices. As part of ongoing education, Angela attends several courses and summits each year to ensure that she stays on top of compliance issues as they are happening. She and the CentraVance team are more than ready to provide your business and/or practice with the comprehensive compliance training it needs. Angela and the CentraVance team will help your small business be fully dressed and prepped for test day!

CHAPTER FOUR

What To Do After A HIPAA Violation

CHAPTER FOUR

What to do After a HIPAA Violation

Growing up, my favorite excuse to get out of trouble was “But Dad, I didn’t know.” It was second only to “But Mooooom, I didn’t think...” I am not quite sure why I liked these excuses. They NEVER worked. Ever. And they don’t work today when my kids try them with me. I hear my Mom’s voice come out of my mouth when I tell a child, “You not thinking is half the problem.” Well, guess what? These excuses don’t fly with the Department of Health and Human Services when it comes to HIPAA violations either. A defense of “we didn’t know” is no defense at all.

Thankfully, most medical and dental practices take great care to ensure that HIPAA Rules are followed and violations do not occur. But let’s face it: mistakes happen. Monitors get left unattended and suddenly patient information is visible to the waiting room. A USB containing patient information gets lost. An email gets sent to the wrong person. All accidents. And yet all HIPAA violations. So, what’s next? What happens after HIPAA violations largely depends upon the severity of the violation.

Civil penalties for HIPAA violations start at $100 per violation by anyone who violates HIPAA Rules. The fines can rise to $25,000 to 1.73 million dollar range if there have been multiple violations of the same type or when the individual was aware that HIPAA Rules were being violated or should have been aware had due diligence been exercised. If there was no willful neglect of HIPAA Rules and the violation was corrected within 30 days from when the employee knew that HIPAA Rules had been violated, civil penalties will not apply. Therefore, it is imperative to have policies and procedures in place and that all employees are well trained. Employees need to know that should an incident occur, it should be reported and addressed immediately. Furthermore, healthcare organizations are not permitted to take retaliatory action against individuals who report a HIPAA violation in the workplace.

The possibility for fines and litigation are reduced if proper compliance was sought both before and after the discovered violation. For example, was the staff trained properly? Were there plans and policies in place prior to the violation? Was the violation reported to the proper people once discovered? Was the incident accidental, due to negligence, or something more nefarious? Simply put, was due diligence exercised?

This is where a compliance officer or 3rd party objective consultant like CentraVance can really save your practice! He or she will be better able to help your practice work through the required risk assessment, give sound advice on the nature of the incident, and instruct you on what steps to take in order to protect your practice's reputation. This is particularly important if the incident is determined to require breach reporting and notification to the patient(s) and Health and Human Services.

All incidents are documentable, but not all will be reportable. You must complete a risk assessment to help determine the level of compromise.

There is a minimum of 4 factors to be considered when conducting a risk assessment:

- The nature and extent of the Patient Health Information (PHI) involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

If there is a higher probability of compromise based on the above four factors, notification is required. Entities must consider what was inappropriately disclosed, to whom it was disclosed, whether that person saw the data, and what methods of mitigation were available. Additionally, when these mistakes happen, be they through simple human error or something more calculated, HIPAA requires us to train and retrain when things go wrong to help us not make the same mistakes over and over.

There is probably no way for me to escape turning into my mother. It's gonna happen. I'm three years away from yelling at kids to get off my lawn. But there is hope for your healthcare practice. Call the team at CentraVance Consulting to make sure you have the proper policies and procedures in place and your team is trained to avoid HIPAA violations. They can also help you mitigate any HIPAA violations that may have occurred and empower you to protect your brand, your patients, your employees, and your practice's reputation.

CHAPTER FIVE

Budgeting for Compliance

CHAPTER FIVE

Budgeting for Compliance

Healthcare practices can easily underestimate the investment required to meet compliance. Thinking compliance is a one-and-done activity that you can navigate with minimal spending only sets you up for unpleasant surprises later on. Compliance can be a long, drawn-out process, involving HR, finance, security, leadership, and others. Therefore, it's important to look at all the costs up front in order to set a realistic budget.

Compliance costs should be viewed as a return on investment. Training employees, implementing policies and procedures, assessing risks, managing risks, improving technical infrastructure are all a part of protecting a practice's brand and reputation.

Let's begin by breaking down the various types of costs associated with compliance:

•**Direct Costs:** These are expenses related to implementing compliance requirements, including and enterprise-wide HIPAA security risk assessment, auditors, and new technology.

•**Indirect Costs:** These are the intangible costs like time, management, and training.

•**Opportunity Costs:** There are also costs to consider if you don't meet compliance, such as lost business, penalty fees, and a diminished reputation in the industry.

The actual costs for each of these categories will vary based on:

•The industry your organization sits in

•How many employees you have

•The number of regulations you're required to adhere to

•The amount of sensitive and confidential information you're required to safeguard

Let's look at which personnel may be involved in establishing HIPAA compliance for your healthcare practice. Many times, companies only take into account the cost of hiring an outside contractor to help with the compliance process, but you should also take into account which internal team members will be involved. Typically, it's representatives from IT, legal, security and/or compliance, HR, finance, and accounting.

You should also factor in additional time and resources to implement and maintain compliance processes and technologies across the practice. For some healthcare entities, maintenance alone can take one day a week, if not more, depending on company size. Keep in mind that compliance is never just a one-time thing. As we have written about before, training must occur at the time of hiring new personal a well a annually. Be sure to address this in your budget.

The hard costs are ultimately just half of the compliance equation. What is the cost to you if you decide not to become compliant? You may be looking at hefty fines, loss of customers, reputation damage in the industry, and so on. For many companies, compliance is a necessity to patients and clients.

Roy Snell, CEO of the Health Care Compliance Association, a member-based association for compliance professionals in the healthcare provider field, said, “Organizations that have effective compliance and ethics programs attract and retain good staff and are more trusted by their communities and potential customers. Good compliance and ethics programs have an impact on revenue that must be considered when you calculate cost. Trusted companies get more revenue than companies that can’t be trusted.”

The bottom line is that an entity will pay for compliance one way or the other: either proactively as a part of their business model and assurance to their patients that they will protect the privacy and security of the information we collect on patients, or reactively – which costs more money, stress, and potential loss of business when regulators become involved because of a bad outcome or violation of rule. At that point, we must spend the money on our compliance programs, on consultants, attorneys, and for fines and penalties that may be assessed for non-compliance.

For a better idea about how to get started on insuring you protect your practice’s HIPAA health and reputation, contact Angela and her team at CentraVance consulting today!

CONCLUSION

Hiring a Compliance Expert

CONCLUSION

Hiring a Compliance Expert

Unless a practice has the resources to hire compliance professionals (as employees) to manage their compliance programs, it is ALWAYS best practice to do your research and find experts in the areas of compliance your practice falls under. Office managers and administrators wear many hats and must be experts in patient and employee management. They also have to manage vendor relationships, revenue cycles, insurance issues.

It is nearly impossible for one person to be the master of all things. Hiring a 3rd party expert helps ensure compliance with the rules, and support during crisis management. Just having a resource to ask questions about what to do when faced with an incident, a complaint, engaging a new business associate would prove to be invaluable.

CentraVance Consulting, LLC was founded by Angela Simmons in 2017 with a single mission: to help clients meet their complex industry compliance requirements. By providing superior service and support through education, consulting and project management, we want to be a partner, not just another vendor.

With more than 22 years of healthcare experience, Angela Simmons has worked as a Certified Dental Assistant and a Dental Assisting Educator/Director with the North Carolina Community College System and served as a Consultant for the Commission on Dental Accreditation. She received her Bachelor of Science in Health Services Management from East Carolina University. Passionate about compliance, and most especially HIPAA, Angela is a Certified HIPAA Professional (CHPC) and a Certified Cyber Security Architect (CCSA). Angela's clinical, managerial and teaching experience make her a great choice to provide employee safety and patient privacy training for CentraVance clients. Her experience in both the clinical and educational settings provides her the insight and ability to identify safety and privacy issues that can occur in both medical and dental offices. As part of ongoing education, Angela attends several courses and summits each year to ensure that she stays on top of compliance issues as they are happening. She is currently an active member of the Healthcare Compliance Association.

Reach Out today for a Free Risk Assessment!

CentraVance

www.centravance.com

ask.us@centravance.com

804-977-1201