Review of Optometric Business

5 SIMPLE THINGS ODs CAN DO TO ADDRESS THEIR HIPAA COMPLIANCE

BY Compliancy Group

5 SIMPLE THINGS ODs CAN DO TO ADDRESS THEIR HIPAA COMPLIANCE

BY COMPLIANCY GROUP

HIPAA compliance can be complicated when you try to go it alone.

Between changes to regulatory requirements and heightened enforcement efforts, HIPAA compliance is a moving target of "rights and wrongs" that all health care providers must address within their practice. Doctors of optometry are more exposed to the risk of a HIPAA violation than ever before if they aren't addressing their HIPAA compliance.

At Compliancy Group, we've been providing educational HIPAA resources since 2005. It's out mission to help health care providers simplify their HIPAA compliance, which is why we've put together this eBook. We're the endorsed HIPAA compliance solution of eyecare professionals across the country--and we're proud of our commitment to helping eyecare succeed. Our HIPAA compliance software is web-based and gives our users everything they need to confidently satisfy their HIPAA requirements—including a dedicated coach to walk them through every step of the way.

We've put together this simple guide to give you and your practice a head start on your compliance program with five steps you can take right now to start addressing your HIPAA requirements. The important thing to remember about HIPAA compliance is that it's not a check-the-box exercise. You need to fulfill your requirements under the law to keep patient information safe and secure—and this guide will give you what you need to get started.

This is by no means a definitive guide to creating a total compliance program. Instead, we've narrowed down a list of five things we see ODs struggling with in regards to their compliance. This eBook will allow you to easily learn how to address some key components of an effective HIPAA compliance program within your practice.

What is an Effective HIPAA Compliance Program?

Creating a HIPAA compliance program requires dynamic precision. You need to ensure that your compliance program addresses the current needs of your business, while allowing for unforeseen circumstances that may arise, such as a data breach, natural disaster, or unauthorized disclosure of protected health information (PHI, any demographic information that can be used to identify a patient).

The important thing to remember about HIPAA compliance is that the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) outlines that HIPAA covered entities (including health care providers such as ODs) must implement an "effective" compliance program. OCR has issued guidance on this issue in the form of seven fundamental elements.

What is HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. The regulation is composed of a series of rules that have been enacted over the years in order to account for changes to patient privacy needs and advances to security technologies. Collectively called the HIPAA Rules, these set national privacy and security standards for the maintenance and protection of sensitive health care data that all health care professionals must adhere to.

Seven Fundamentals of an Effective Compliance Program

1. Implementing written policies, procedures, and standards of conduct.
2. Designating a compliance officer and compliance committee.
3. Conducting effective training and education.
4. Developing effective lines of communication.
5. Conducting internal monitoring and auditing.
6. Enforcing standards through well-publicized disciplinary guidelines.
7. Responding promptly to detected offenses and undertaking corrective action.

SOURCE: Department of Health and Human Services, https://www.oig.hhs.gov/authorities/docs/03/050503FRCPGPharmac.pdf

Notice that the Seven Elements do not list specific items such as "Implement ABC email encryption services" or "Purchase an XYZ alarm system." Instead, you find a general list of pieces of a compliance program that are fully scalable regardless of the size and scope of the health care practice in question. Creating an effective compliance program means implementing processes that work for the unique needs of your practice, all while satisfying federal privacy and security standards outlined in the regulation.

Compliance and Security

Compliance is a delicate balance of administrative policies and cyber-security safeguards. ODs need to address BOTH to keep their practice safe. This ebook gives readers a rundown that covers both administrative and practical steps that can be taken right now to improve HIPAA compliance.

The benefits of HIPAA compliance come from protecting your practice from data breaches and fines, but can go much further. HIPAA compliance allows your practice to increase patient loyalty, better your quality of care, and differentiate yourself in a market full of online competitors. By demonstrating to your patients that you care about the privacy and security of their data, you're giving them confidence in your services and making them more likely to return to you, rather than rely on a start-up web app or service provider.

On the following pages, we discuss the top five things you can implement in your practice right now to begin addressing some of your HIPAA compliance requirements. Read on for actionable tips and measures you can take to improve the privacy and security of your health care data.

EMPLOYEE TRAINING

When it comes to HIPAA compliance, employee training is one of the most important pieces of an effective compliance program. Employee training can mean the difference between a major HIPAA violation, and keeping your practice safe.

HIPAA regulation requires that your practice conduct annual employee training for all staff members—including doctors. However, it's important to remember that one-off annual training sessions are not considered effective under the regulation. Let's consider this scenario to illustrate why. If you conduct your annual HIPAA training on a Monday, then have a new employee join your practice the very next day, that new employee will have missed their chance to receive HIPAA training for an entire year. That means that for the full year that they work for your practice, they will be untrained on HIPAA compliance and on your practice's policies and procedures. This becomes a liability that could ultimately result in your practice being held responsible for a HIPAA violation caused by this employee.

In order for HIPAA training to be effective, it must be conducted on an ongoing basis, preferably wrapped-up into your onboarding process for new employees.

Additionally, there are several different types of HIPAA training that your practice must undertake each year. These include:

HIPAA 101 Training: Effective HIPAA training must include the fundamentals that you and your staff need to know about the ins and outs of HIPAA compliance. HIPAA 101 training should give you an overview of what HIPAA regulation is, what your responsibilities are toward maintaining PHI, and what is required for HIPAA compliance. HIPAA 101 training is meant to give you confidence in how your business handles PHI and safeguards the privacy and security of your patients' health information. Annual HIPAA 101 training is an essential way to prevent possible breaches and fines before they occur and is mandated by HIPAA regulation.

Cyber-Security Awareness Training: Because health care data is increasingly digital, it's more important than ever before for ODs to train all staff members on proper cyber-security awareness. This includes training on issues such as phishing scams (e.g., when a fraudulent email containing a malicious link is sent to infect your system), ransomware, malware, and data breach prevention. Cyber-security awareness training should be carried out quarterly to keep your staff educated on the most up-to-date information regarding cyber threats to your practice.

Policies and Procedures Training: Another essential element of HIPAA compliance is the creation, documentation, and implementation of policies and procedures. HIPAA policies and procedures must directly apply to all applicable HIPAA standards that your practice is responsible for complying with. ODs must ensure that all employees have been properly trained on the content of these policies and procedures. Policies and procedures are meant to be unique to the needs of your business (just another reason why policy binders don't work).

SOCIAL MEDIA POLICIES, PROCEDURES, AND SAFEGUARDS

HIPAA and social media use can lead to some of the most common misunderstandings that optometric professionals face. Employees who aren't properly trained on HIPAA and social media can expose your organization to potential HIPAA violations and costly fines.

Whether your practice is using Facebook to attract new clients, or your employees are posting about their workday on Twitter, improper use of social media can lead to major problems for healthcare professionals.

The question becomes: how can healthcare professionals use social media without violating HIPAA privacy and security requirements?

What Can You Post on Social Media?

When it comes to HIPAA and social media, the most important thing to remember is that social media content should NEVER include information that can be used to identify individual patients or their medical records. This kind of data is considered Protected Health Information (PHI) under HIPAA.

PHI is any demographic information that can be used to identify one of your patients. This includes names, full face photos, dates of birth, addresses, social security numbers, medical data, and financial information, among others. PHI is strictly protected under HIPAA regulation, outlined in both the HIPAA Privacy Rule and the HIPAA Security Rule.

Who Enforces HIPAA Regulations?

HIPAA regulation is created by the Department of Health and Human Services (HHS). The HHS Office for Civil Rights (OCR) is the enforcement arm for HIPAA. OCR is responsible for investigating reported HIPAA violations, auditing health care businesses for potential violations, and ultimately issuing financial penalties, settlements, and fines for HIPAA violations.

HIPAA regulation forbids the use of PHI in marketing or social media campaigns, so this should be avoided at all costs to protect your patients' privacy.

But that doesn't preclude your practice from having a social media presence. Creating social media accounts for your practice is actually a very effective way to attract new clients and advertise your services.

Below, we list some of the things you can post on social media:

- Health tips that patients might find useful

- Upcoming events patients might like to attend
- New research or findings related to your field
- Honors or awards your organization has been granted
- Profiles or bios of your staff
- Advertisements of your services as long as they DO NOT CONTAIN THE PROTECTED HEALTH INFORMATION of any of your patients (including names, photos, or any other personally identifiable information)
- Discounts or special offers on services you provide

Your practice should have HIPAA policies and procedures that document these restrictions and exceptions on content that may be posted to social media accounts. Additionally, your employees should be trained on these policies and procedures, with special focus on social media usage.

Social Media Training: With the presence of social media in the workplace as a marketing tool and for personal use growing, it's never been more important to train your employees on how to avoid HIPAA violations on social media. Effective HIPAA training should introduce your employees to basic ways to handle social media. Pair HIPAA training with your organization's Policies and Procedures to give your employees the tools they need to protect patient and client data.

IMPLEMENTATION STEP

3

ENCRYPTION

Encryption takes your data or electronic protected health information (ePHI) and turns it into unreadable text using software or algorithms. This unreadable text can only be deciphered through an encryption key that will allow you to read it once again. This protects your data even in the event of a breach or theft, and can leave the data useless to anyone who obtains or steals it.

HIPAA regulation identifies two distinct types of data that should be encrypted.

Data at rest is any data stored in an electronic format being stored on a device. Data is effectively "at rest" any time it is not being transferred from one end-point to another.

Data in motion is any data in the process of being transferred. This includes data sent via email or other transfer medium.

Additionally, there are different methods of encryption that your practice should implement to protect data at rest and data in motion.

End-to-End Encryption: HIPAA encryption requirements outline that covered entities, such as ODs, should utilize end-to-end encryption (E2EE) to protect data in motion. End-to-end encryption is a means of transferring encrypted data such that only the sender and intended recipient can view or access that data. This is distinct from other means of data transfer wherein encrypted data is temporarily stored on an intermediary server. If an encrypted data transfer requires that data go through an intermediary server (as is the case with regular email, iMessage, etc.), it is not HIPAA compliant and cannot be used by HIPAA-beholden entities.

Full Disc Encryption: Full disc encryption is a type of encryption that encrypts all data on your entire computer. This is distinct from other types of file encryption, which only isolate and encrypt individual files within your hard drive. Full disc encryption will protect your computer systems from malicious attacks aimed at your sensitive health care data. This is an essential means of HIPAA encryption that is used to protect data-at-rest.

By implementing HIPAA encryption standards within your practice, you're ensuring that the data you handle will be kept safe, even in the event of a data breach or malware incident. And when it comes to transferring data between providers, or even from provider to patient, having the proper encryption safeguards in place will protect that data from being intercepted by unauthorized parties.

IMPLEMENTATION STEP

4

PASSWORD PROTECTION

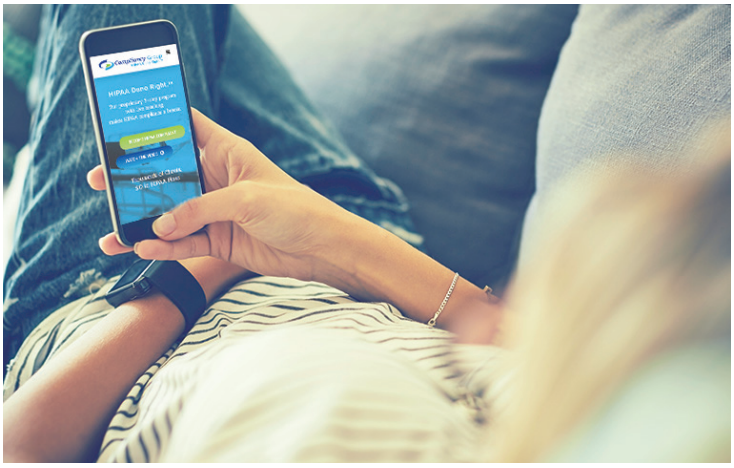
HIPAA compliance calls for password management and protection safeguards in order to protect ePHI. That means that if your practice uses digital, cloud, or electronic storage devices, and particularly electronic health record (EHR) or electronic medical record (EMR) systems, then you must have password protections in place to ensure that access to that data is kept safe and secure.

Password management is one of the best practices that ODs can use while trying to create an effective compliance program. HIPAA password protection standards are based off of NIST (National Institute of Standards and Technology) protocols. NIST releases security guidance on an ongoing basis to highlight industry best practices. NIST also routinely issues new guidance on password creation, which you should implement to keep your data safe.

Here are a few of the measures that you can put in place to keep passwords compliant with NIST and HIPAA requirements:

- **Use a minimum of 8 characters:** NIST also says that passwords can be up to 64 characters long if it's protecting particularly sensitive data.
- **Avoid password hints:** creating hints such as "my last name" or "my anniversary" can seriously compromise the integrity of your passwords. Avoid these at all cost!
- **Create memorable passwords:** NIST no longer suggests unnecessarily complicated or obtuse passwords. These can actually lead to weaker passwords in the long run. Your password should be sufficiently unique and memorable so as to avoid the dreaded post-it note on the computer monitor.
- **Vet passwords against a list of common/weak options:** NIST guidance suggests that passwords should be vetted against a list of common passwords (such as "password," "123456789," "ChangeMe," and so on). This can be executed by an IT or security firm.

By implementing password management safeguards, you're helping to avoid unauthorized access to ePHI that can result in major HIPAA violations and potential data breaches.



MINIMUM NECESSARY ACCESS

The Minimum Necessary Rule is part of the HIPAA Privacy Rule. The Privacy Rule governs the use, distribution, and access to PHI both by health care professionals and by patients themselves.

The Minimum Necessary Rule states that covered entities—including ODs—can only access, transmit, or handle the minimum amount of PHI that is necessary to perform a given task. That means that sending entire copies of a patient's medical record via email, when only part of it is relevant to the task at hand, is a violation of this Rule. The Rule is in place to mitigate the potential damage that can result from a data breach. Even though, ideally, the goal is not to experience a data breach at all, in the event that it does occur, the Minimum Necessary Rule is meant to limit the impact on a patients' privacy.

The Minimum Necessary Rule also intersects with access controls. The Privacy Rule states that access to PHI should be limited based on the role being performed and by the employee in question. Therefore, all employees should not have the same level of access to PHI if their organization-based role does not depend on it. Again, this is meant to limit the potential impact of an unforeseen data breach.

Keeping the Minimum Necessary Rule in mind while you go about your operations is a fundamental way you can help prevent data breaches in your organization, all while working toward HIPAA compliance. With the proliferation of EHR and EMR platforms, access to sensitive medical information is easier than ever. And that means the same information is also highly susceptible to ransomware or malware.

By limiting the amount of PHI you access during the course of your work, you can help maintain your patients' privacy and avoid mounting HIPAA violations and fines.

HIPAA: What are the Consequences of Non-Compliance?

Financial penalties for HIPAA violations range from $100-$50,000 per incident, with a maximum fine of $1.5 million per violation. OCR investigators levy HIPAA fines based on the level of "perceived negligence" uncovered during an investigation. That means that if your practice is aware of your responsibilities toward HIPAA compliance, but fail to address what the law requires, you could be found "in willful neglect," and on the receiving end of hundreds of thousands of dollars in fines.

PUTTING IT ALL TOGETHER

At the end of the day, the most important thing to remember about HIPAA compliance is that it is not a check-the-box exercise. The items we've listed in this guide are a great start to your HIPAA compliance program. But a truly effective HIPAA compliance program must address all Privacy and Security standards listed in the regulation.

When you're creating the rest of your HIPAA compliance program, make sure that you have solutions in place to address:

- **Self-Audits** An effective HIPAA compliance program requires that you audit your practice against the HIPAA Rules. This gives you a baseline of your deficiencies that you will have to address.
- **Remediation Plans** In order to mitigate HIPAA violations, your HIPAA compliance program must include actionable plans to remedy the deficiencies identified in your self-audits.
- **Policies, Procedures, Employee Training** HIPAA policies and procedures must be updated annually, and your HIPAA compliance program should be dynamic, giving you the ability to both craft and review them as time goes on. Additionally, all staff members must be trained on policies and procedures year after year, as discussed above.
- **Documentation** Documenting your progress is perhaps the most important component of HIPAA compliance management. Documentation must be retained for six years as per federal regulation.
- **Business Associate Management** Managing vendors with whom you share PHI is an essential component of HIPAA. Your HIPAA compliance program should include Business Associate Agreements, executed with vendors before any PHI is shared.
- **Incident Management** Although you hope that your practice will never experience a data breach or HIPAA violation, sometimes they can occur. Another essential component of HIPAA compliance management includes tracking, investigating, and reporting these data breaches to HHS as they occur.

HIPAA Compliance Software
Compliancy Group

Compliancy Group

HIPAA should be simple. That's why Compliancy Group is the only HIPAA software with expert Compliance Coaches® holding clients' hands to simplify compliance. Compliancy Group gives eyecare professionals confidence in their compliance plan, increasing patient loyalty and profitability of their practice, while reducing risk.

Compliancy Group is proud of its dedication to helping eyecare professionals across the country succeed. Compliancy Group is a proud sponsor of Think About Your Eyes and has been a visionary-level contributor to the AOA PAC since 2015. Compliancy Group is also the endorsed HIPAA compliance solution of AOA Excel.

Compliancy Group's Compliance Coaches field questions and guide users through implementing an effective compliance program, built to address the full extent of HIPAA regulation.

With Compliancy Group, eyecare professionals can focus on running their practice while keeping their patients' data protected and secure.

HIPAA SEAL OF COMPLIANCE
COMPLIANCY GROUP
HIPAA VERIFIED

Find out more about how Compliancy Group and the HIPAA Seal of Compliance® can help simplify your HIPAA compliance today!

Visit www.compliancygroup.com or call 855-854-4722