What is HIPAA Compliance and How to Get Started?

Jotform

jotform.com/hipaa/

This page was intentionally left blank.

What is HIPAA Compliance and How to Get Started? 0

Introduction 3

Why is HIPAA compliance crucial? 4

HIPAA compliance enforcement 5

What rights does HIPAA grant patients? 6

What is patient confidentiality, and how does it affect your practice? 8

Becoming HIPAA-compliant: Where to start 10

Why forms that enable HIPAA compliance are essential to your practice 11

What are the HIPAA security safeguards? 12

Best email providers that enables HIPAA compliance 12

Once your email is secure, what can you do about storing data securely? 13

Best cloud storage and file sharing services for HIPAA compliance 13

Best physical safeguards you can take to protect PHI 14

What are the requirements for servers for HIPAA compliance? 15

Patient confidentiality laws and HIPAA 16

What actions are considered a HIPAA violation? 17

Sanctions of HIPAA violations 18

Civil penalties 18

Criminal penalties 19

How to identify your risk level 20

HIPAA training essentials 21

How to conduct HIPAA training 22

How often should you provide HIPAA training? 22

How to be HIPAA compliant on social media 23

The first step in HIPAA compliance: Intake forms 23

How to improve your patient intake process 24

How to keep patient intake forms secure 24

Specific intake form cases 25

Introduction

Each year, 12,000 HIPAA compliance complaints require action. Of the approximately 230,187 private medical practices in the United States, all face the challenge of maintaining HIPAA compliance.

Data privacy is no longer as simple as locking a file cabinet. Technology has made it easier for healthcare data to be stolen, leaked, and misused. This vulnerability is why you and your employees need to understand what HIPAA (the Health Insurance Portability and Accountability Act) is and how you can stay compliant.

Here's what you need to know to keep patients and your practice safe, including why you need forms that enable HIPAA compliance.

Why is HIPAA compliance crucial?

"HIPAA compliance is a multitiered issue that is made up of three main pillars. These pillars are designed to identify and mitigate risk on an ongoing basis."

— Dr. Danika Brinda, President/CEO of Planet HIPAA

First things first, we need to understand who HIPAA applies to. Put simply, healthcare providers and their partners are bound to HIPAA law, as well as related legislation such as the HITECH Act and the HIPAA Omnibus Rule. The law requires that healthcare providers and their partners take every precaution to keep protected health information (PHI) safe, whether it's physical or electronic.

Protecting health information wouldn't be so difficult if healthcare practices could safely collect it, store it, and "throw away the key." But modern medical, dental, and other healthcare practices don't have that luxury. After all, protected health information isn't static.

Staff members frequently retrieve and update protected health information. PHI changes hands between treating physicians, pharmacies, insurance companies, patients, and sometimes a patient's legal representatives. Office staff also handle printed copies of protected health information.

Every healthcare organization must have clear protocols to keep patient data safe. They also need the necessary technology to comply with HIPAA law and avoid violations.

HIPAA compliance enforcement

HIPAA violations care hefty fines. Who enforces HIPAA? The U.S. Department of Health and Human Services (HHS) has delegated all HIPAA enforcement to their Office for Civil Rights (OCR). With a hefty annual budget of over $32 million, this department gets results. If you're not complying with HIPAA, they'll find out and you will face the consequences.

Enforcement by the OCR includes three primary functions:

- Investigating complaints filed by individuals
- Conducting compliance reviews of those who manage protected health information
- Providing education, outreach, and resources on staying compliant

The OCR describes someone who manages protected health information as a "covered entity." When reading HIPAA laws, you'll repeatedly see this term. Every mention of a covered entity refers to you and your practice.

An investigation into a covered entity, like your practice, may result in one of three outcomes:

1. The OCR finds no violations.
2. The OCR obtains voluntary compliance, corrective action, or other agreement.
3. The OCR issues a formal finding of violation.

Since the HIPAA Privacy Rule began to be enforced in 2003, the Office for Civil Rights has handled nearly 200,000 complaints with a 96–percent resolution rate. Its success makes the OCR potentially one of the most efficient and effective government entities in the United States.

While government regulations might conjure up dystopian imagery of Big Brother watching over your shoulder, they serve an essential function. In effect, HIPAA enforcement by the Office for Civil Rights has increased the rights of patients in the United States.

What rights does HIPAA grant patients?

You might think that HIPAA is a big list of regulations and fines designed to make your life more difficult. But that's not HIPAA's purpose at all. HIPAA is first and foremost designed to protect data and patient rights.

One of these rights is the patient's right to access their health information. Of course, this means you must have systems in place to verify that the person requesting information is, indeed, the patient or a legal representative.

Patients also have the right to inspect or receive a copy of their medical records. They can request that you send those records to another person. There is no time limit for a patient to request information. As long as you maintain protected health information, which is typically retained for seven years, the patient can request it.

Protected health information goes beyond healthcare basics and includes

- Billing information
- Claims processing
- Enrollment status
- Case management, including community services, etc.
- Prior authorization documentation

- X-rays, lab results, and other test and procedure results
- Visit notes

While the covered health information may seem endless, there are some limitations to these requests. For example, HIPAA doesn't give patients the right to certain types of healthcare data:

- Patients can't request logs of information that may include protected health information but are not part of medical decisions. For example, a person can't request a log of their calls with a receptionist or customer service department.

- Patients don't have the right to access psychotherapy analysis notes. This exception maintains the integrity of mental health evaluations. However, the patient does have a right to session notes that are kept separately.

- Patients don't have the right to view notes compiled for legal purposes.

To protect themselves, some medical providers try to bar certain individuals from accessing their information. Others make it unnecessarily difficult to do so. But the regulations require that you balance security and accessibility. For example, medical providers can't impose restrictive policies, such as

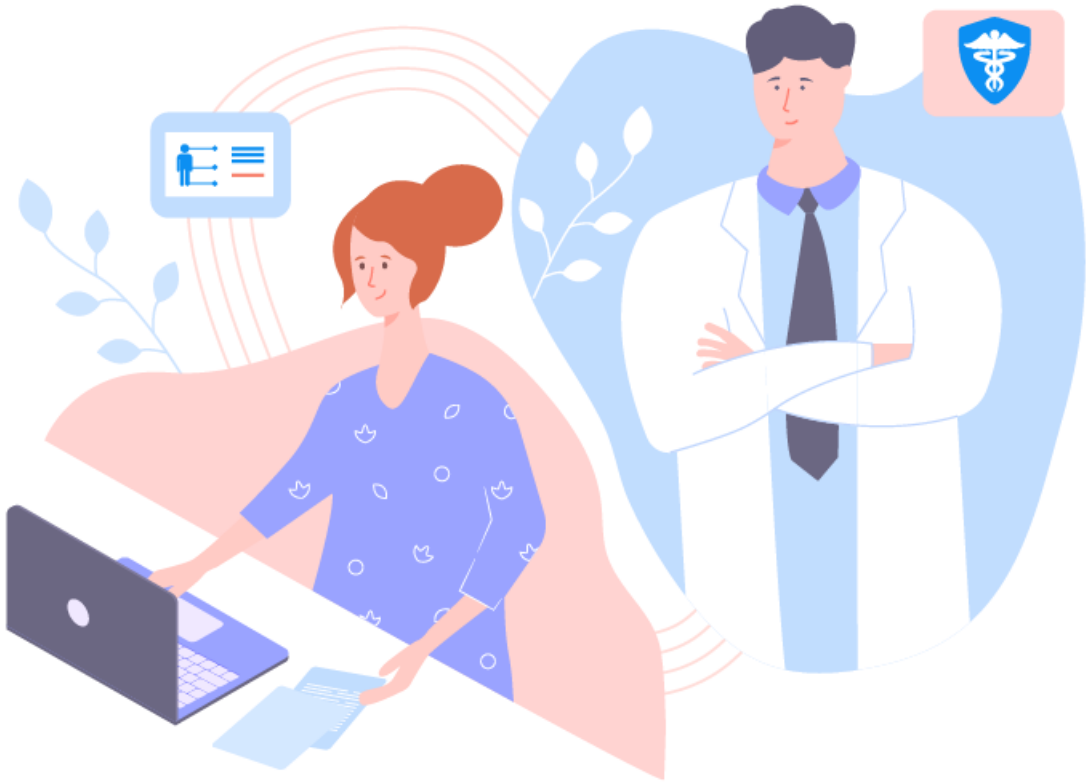
- Allowing access only through an online portal. Patients without internet service would be unable to gain access.

- Requiring everyone to request information in person. Patients who are homebound or live far away would be unable to gain access.

- Sending an authorization form by regular mail when there are faster ways of getting permission. Patients may need to wait an unreasonable amount of time to access protected health information.

The rights granted by HIPAA guarantee patients access to their health information. Enforcement by the Office for Civil Rights makes sure that healthcare providers protect their patients' private data and confidentiality.

What is patient confidentiality, and how does it affect your practice?



The Gale Encyclopedia of Surgery and Medical Tests defines confidentiality as “the right of an individual to have personal, identifiable medical information kept private. Such information should be available only to the physician of record and other health care and insurance personnel as necessary.”

Patients have a right to confidentiality. They rely on you to keep their personal information safe for many reasons. Inappropriate disclosure of protected health information could have negative consequences for your patients.

Public or personal embarrassment

Medical information can be embarrassing. From mental health challenges to strange fungi to STDs, many people have information that they don’t want shared with others.

Job discrimination

If employers had access to health information, how would they use it? If they could get this information in a background check, it could influence hiring and firing decisions. This could easily lead to discrimination. Legally, employers can’t ask about pregnancy or health conditions in an interview. Patients are protected because employers can’t access health records.

Family or legal disputes

Certain protected health information could affect the outcome of a legal dispute, such as using mental health records in a custody battle.

Victim targeting

Certain types of patients are especially vulnerable to having their protected health information misused. For example, patients with a diagnosis of early dementia may be targeted by nefarious financial institutions or fraudsters. People who have chronic conditions could become prey to quacks pushing costly fake cures.

The threat is very real, and patients deserve to have their health information protected.

Loss of trust

One of the most commonly overlooked impacts of breaching HIPAA regulations is loss of trust. New patients may choose to go elsewhere. Existing patients may leave a longtime doctor over safety concerns.

The issue of trust goes back to the core purpose of HIPAA compliance. HIPAA is about protecting the patient, which isn't always as straightforward as you might think.

Becoming HIPAA-compliant: Where to start

Still, everyone has to start somewhere. Perhaps you've been trying to comply but don't know where to begin. You might have discovered things you've overlooked while reading this article.

Here are seven steps that you can use as a HIPAA compliance checklist for your practice:

1. **Take an online HIPAA checkup**. Using an online HIPAA checkup can help small practices quickly identify gaps and risks in their processes. You can then use this information as a baseline to start from. Planet HIPAA's online HIPAA Checkup helps you start down the road toward compliance.

2. **Do a thorough risk assessment.** How can you be HIPAA compliant if you don't know where your weaknesses are? Even if you've done a risk assessment in the past, you may have new information to add. There may be areas of your PHI management that you hadn't previously considered.

3. **Review the Health and Human Services website** for the most recent guidelines. Sign up for updates from the site. Technology is constantly changing. As it does, HHS updates will keep you updated on best practices. This guidance should be thought of as equally important as the law itself. If the Office for Civil Rights audits you, they will be looking at whether you're up to date.

4. **Update your training materials** at least once a year. Most of the material will stay the same, but incorporate any recent HHS updates into the manual. If you've been using the same manual for more than five years, you're way past due for an update.

5. **Schedule annual HIPAA training** for your team. This training isn't something you want to skimp on, so plan a whole day for it. If everyone can't be away at once, consider creating a modular online course. Because this type of course is interactive and includes quizzes, it can also improve your staff's understanding and retention of the material.

6. **Get signed Business Associate Agreements** from any third-party providers, partners, or contractors. BAAs are not optional, so have procedures in place to get them signed before you share any protected health information.

7. **Use software that enables HIPAA compliance** to make managing protected health information easy and secure. Your electronic recordkeeping should include data storage solutions and forms that comply with HIPAA requirements.

Why forms that enable HIPAA compliance are essential to your practice

"Providers need to fill out an average of 20,000 forms every year."

— Rick Hammer, ReferralMD

Due to the considerable amount of recordkeeping required for HIPAA compliance, electronic forms provide many advantages. Unlike written forms, electronic forms are permanent and always legible.

Electronic forms increase the efficiency of your documentation process by eliminating duplicate work. They can ease, or even automate, data collection. They also reduce data entry when interfaced with electronic spreadsheets or medical systems.

When choosing a form service for your practice that helps you become HIPAA-compliant, remember the importance of electronic security. Your forms must use data encryption to ensure that any stolen or leaked data will be unusable. In addition, the connection between the form and the server must be secure.

To learn more about how you can accomplish this level of HIPAA security, centralization, and automation, get forms from Jotform that enable HIPAA compliance.

What are the HIPAA security safeguards?

These days, electronic protected health information doesn't just reside in an isolated computer in someone's office. It's on the internet. It's being transferred from one place to another wirelessly. This transfer is a particularly critical point for ePHI because anytime it's transmitted, it can be intercepted with the right tools.

So how can you transmit information securely? What is data security, and how can you do it correctly?

Encryption is the answer. A system of encoding information, encryption disguises all the information in another form before transmitting it. When the information has safely reached its destination, it is then converted back to a usable form.

Let's look at some of the top software service providers that help with HIPAA compliance.

Best email providers that enables HIPAA compliance

Whether you have employee-to-employee communications or send and receive patient forms and updates through email, your email must be a fortress. Otherwise, email easily becomes a weak link in HIPAA compliance.

You have several great options that are both secure and versatile, so it's easy to integrate them into your existing systems.

Here are the best email service providers that help with HIPAA compliance:

- **Aspida Mail** allows simple yet secure email migration.
- **NeoCertified** provides easy access through a secure portal.
- **Paubox** turns your existing email into emails that help with HIPAA compliance. It works with Gmail and other popular email services.
- **Protected Trust** turns Outlook and other Windows applications into software tools that enable HIPAA compliance.
- **Virtru** offers end-to-end encryption and fully integrates with software you already use, like Microsoft and G Suite.
- **VM Racks** offers standalone email and hosting services that enable HIPAA compliance.

Once your email is secure, what can you do about storing data securely?

Best cloud storage and file sharing services for HIPAA compliance

"91% of healthcare practices are using cloud-based services, yet 47% are not confident in the ability to keep data secure in the cloud."

— *Entech*

Cloud storage offers the flexibility to store large amounts of data without continually having to upgrade your computers. While they excel at convenience, most cloud services only take minimal precautions to keep information safe. They aren't intended for protected health information, financial information, or other highly sensitive data and could pose a security risk.

Box, Carbonite, Dropbox, Google Drive and Microsoft OneDrive are among the top cloud storage and file-sharing solutions for HIPAA compliance.

After securing your data, next you should consider which software tools that enable HIPAA compliance you'll need to use in your practice.

Note that you may need a variety of software. From office suites to specialized forms, healthcare providers must use software that offers HIPAA compliance. These software programs include fax services as well.

Best physical safeguards you can take to protect PHI

Software can take security to an extreme degree. But human error can weaken even the toughest security measures. If you have people sharing passwords, staying logged in indefinitely, or setting up the HIPAA safety components incorrectly, software won't protect you.

Take simple precautions in the office to make all the extra security worthwhile:

- Make things easy but secure. If keeping things secure is too hard, people will create workarounds that put health information at risk. User-friendly systems should always be part of keeping patient data safe.
- Post HIPAA reminders conspicuously around work areas. Move them around periodically so that people are more likely to see them.
- Point monitors away from general access areas. Purchase screen covers that obscure the screen from someone not sitting directly in front of it. It doesn't take Ocean's 11-style planning to pull off this kind of data heist. These days, anyone can easily pull out a smartphone and zoom in on computer screens to capture data.
- Require employees to use strong passwords and to change their passwords regularly.
- Don't allow people to share passwords.
- Force system updates after asking employees to update them voluntarily. An uninstalled update represents a security threat.
- Only allow protected health information to be transmitted to or from your practice using encrypted forms.

With the basic safeguards ready, what are the next steps in becoming HIPAA compliant?

What are the requirements for servers for HIPAA compliance?

Any server your practice uses must enable HIPAA compliance. It could be your primary server, a cloud backup, your email provider, or the server that hosts your website. If it will store or transmit protected health information, it must be compliant. And, you guessed it: You need a signed business associate agreement from the organization that runs it.

For any server to enable HIPAA compliance, it must do more than just keep ePHI safe. It should

- Provide reports that permit a thorough risk assessment
- Create unique logins for each user with associated file access permissions
- Log users off automatically after a certain span of inactivity
- Track individual users' activity
- Encrypt data during transmission and while at rest
- Prevent improper alteration or destruction of files
- Offer an emergency access procedure

Patient confidentiality laws and HIPAA

"HIPAA has helped to streamline administrative healthcare functions, improve efficiency in the healthcare industry, and ensure protected health information is shared securely."

— *HIPAA Journal*

When it comes to HIPAA, ignorance is definitely not bliss. While erring on the side of caution is smart, excess caution could delay patient care.

To balance confidentiality with patient care, it's important to get familiar with some commonly overlooked parts of the law.

Here are some patient confidentiality related HIPAA security rules. Just keep in mind that failure to follow these rules can land your practice in very hot water.

What actions are considered a HIPAA violation?

What are the most common cases of HIPAA violations that result in penalties? You may be surprised by the answer.

According to HIPAA Journal, the most common HIPAA violations are the result of

- Failure to do a complete risk analysis
- Improper disclosure of protected health information
- Delayed breach notification when data breaches occur
- Failure to encrypt electronic health information
- Failure to obtain a business associate agreement

These violations may seem obvious and easy to avoid, but you may not realize how easy it is to get a BAA-related violation. In fact, many practices don't realize how many third parties they authorize to access their information just by using a computer in their practice. This includes allowing a computer program, cloud service, or other technology to collect, store, process, analyze, retrieve, or distribute health information.

Sanctions of HIPAA violations

If your practice violates HIPAA, you might not only face fines. Certain HIPAA offenses can even lead to time in prison.

Civil penalties

The fines are broken up into four tiers that generally represent the extent to which you knew that your actions were illegal:

- **Tier 1: $100–$50,000 per violation ($1.5 million per year maximum).** You didn't know that a violation had taken place. Even if you had done your due diligence, you wouldn't have known. You can't avoid fines completely, but they could be lower. This tier was added to encourage thorough risk assessment to uncover possible risks.

- **Tier 2: $1,000–$50,000 per violation ($1.5 million per year maximum).** The Office for Civil Rights has reasonable cause to believe that you knew or should have known about the violation if you were doing due diligence.

- **Tier 3: $10,000–$50,000 per violation ($1.5 million per year maximum).** You willfully neglected the rules. Once the violation was discovered in an internal or outside audit, you corrected it within 30 days.

- **Tier 4: $50,000 per violation ($1.5 million per year maximum).** You willfully neglected the rules and made no effort to fix the error within 30 days of finding the violation.

A violation is defined as “a single patient record.” In other words, one very bad mistake could represent hundreds or thousands of violations. Could your practice handle a $50,000 hit? What if 1,000 records were compromised?

Most practices can’t survive these kinds of penalties. That’s why being HIPAA compliant is so important. HIPAA compliance means being proactive so these worst-case scenarios never happen to your practice.

Criminal penalties

If a person defies HIPAA in order to harm others, make a profit, or obstruct justice, they can expect the long arm of the law to come down hard on them. If someone collaborated with another person to cover up HIPAA violations, they could be charged with aiding and abetting or with conspiracy. In these cases, the Office for Civil Rights turns you over to the Department of Justice for a federal investigation.

That’s serious business.

A conviction would completely destroy your chances of ever working in the medical field again in any capacity. It could even hinder you from getting any form of employment where integrity is important.

Like civil penalties, criminal penalties are also divided into tiers:

- The lowest criminal penalty is up to **$50,000 and up to a year in prison.**
- You could face **$100,000 and up to 5 years in prison** if you conspired to break HIPAA law by lying about your right to access the information.
- The criminal penalty goes up to **$250,000 and up to 10 years** if you access protected health information with the intention to influence a court case, sell it on the black market, or ruin a person’s life by sharing it on social media.

In addition to criminal penalties, any victims may be able to sue you directly for damages.

How to identify your risk level

The Health and Human Services website provides guidance in determining your HIPAA risk level. But they acknowledge that no two practices are alike or have exactly the same risks.

It's up to you to know your risk level by conducting a thorough risk analysis.

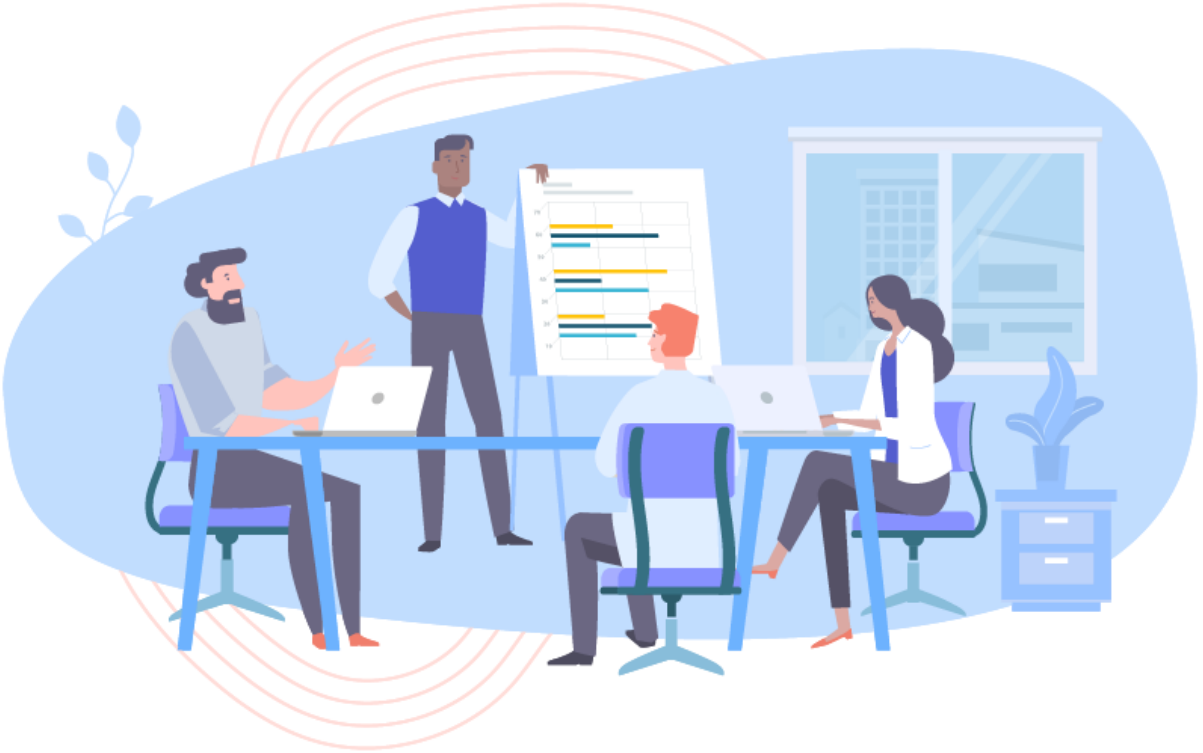
Identify PHI and ePHI in your practice

Where is health information being uploaded, stored, or transmitted? Anything that potentially links a patient to your practice is protected health information even if it doesn't include medical information. Don't disregard physical PHI just because you have paperless medical records. Protected health information can pop up in unexpected places. For example, one small psychology practice in New Jersey was sending copies of billing information to a collections agency that worked for them. An audit revealed that the bills included procedural and diagnostic codes along with insurance information. So make sure to look everywhere for PHI during your risk assessment.

HIPAA training essentials

HIPAA states that training should be provided "as necessary and appropriate for members of the workforce to carry out their functions."

Do you need to educate your cleanup crew about HIPAA compliance? Not likely. But most employees in your practice will manage patient data in some way. Many of them won't necessarily be medical professionals. If they previously worked outside of the healthcare field, they may have never even heard of HIPAA before.



Those who need training could be in a variety of departments, including

- Billing
- Bookkeeping
- Insurance authorizations
- Office management
- Reception
- Data entry

Don’t forget your temporary workers. If you hire from a staffing agency, the temporary employee must sign a business associate agreement since they aren’t your employee. If this contract worker will access PHI, you need to give them some HIPAA training.

How to conduct HIPAA training

You can obtain online certifications or create your own program. Learn the security rules and share them with your team.

The Health and Human Services website offers information on every aspect of the law. It’s mostly in everyday language, rather than legal jargon, so that it can be understood by the average person. But don’t think you can just send someone to the HHS website and tell them to learn the rules.

Formal training is essential for all employees. Your training should answer questions like

- What is HIPAA compliance?
- What is PHI?
- How am I responsible for protecting PHI?
- How do I properly follow procedures?
- How do I use technology to safeguard PHI?
- What physical safeguards should I take?
- What are the penalties for the organization and me if I fail to safeguard PHI?

How often should you provide HIPAA training?

HHS requires you to provide training to every new employee or contract worker within a “reasonable time.” That’s a vague timeline. Yet, considering the importance of HIPAA, it should be the first thing a new employee learns. You may have some wiggle room when hiring clinical staff who have worked in the medical industry, but don’t wait too long. You must be able to show that training was completed within a reasonable period of time.

You are then required to retrain employees “periodically.” Again, that’s vague. Most practices interpret this as annually.

Keep in mind that HIPAA does change as new risks arise and technology changes. You should periodically review new guidance from the HHS site. Keep your training program and employees up to date with any changes.

How to be HIPAA compliant on social media

Social media platforms, both personal and professional, play a large role in the life of your employees. Sharing information about everyday matters, including work, is the norm. But employees who share PHI on social media will leave your practice open to steep penalties. So make sure your employees know what can't be shared on social media.

The first step in HIPAA compliance: Intake forms

Although there are several types of HIPAA compliance forms, intake forms are the cornerstone of protected health information in a practice. The vital information that they contain enables you to better treat your patients. But you are also responsible for protecting that information.

Getting electronic signatures and verifying patient information can all be squared away before the patient walks into the waiting room. If using electronic intake forms is as easy as sending an email, why don't all practices use them? What else should you do to improve the intake process for your patients?

How to improve your patient intake process

Creating the right patient intake process isn't rocket science, but it does take some planning and the right tools.

To improve your patient intake process

- **Get rid of outdated paper forms.** Smart forms, like those from Jotform, make the transition smooth.
- **Streamline your communication.** It's not the '90s anymore, so why are so many practices playing phone tag with patients and using appointment reminder cards? Start identifying the steps in your process that waste the most time. Then, look for an automated solution.
- **Reinforce the patient experience.** How many times have you gotten a bad review that had nothing to do with the actual care you provided? The front desk experience is as important as the healthcare you provide. Make sure everyone in your office is up for the challenge. Have reliable systems in place to help them provide exceptional care throughout the patient experience.

How to keep patient intake forms secure

With the barrage of data breaches in the news, many think that electronic equals unsafe. However, when set up correctly electronic records are far more secure than traditional paper records and file cabinets.

Jotform's electronic forms use extreme measures to keep patient intake forms secure and help you stay HIPAA compliant.

Specific intake form cases

A massage therapy business can use intake forms to gather information just like any other healthcare provider. Beyond that, massage intake forms can help you build a relationship with the patient.

A second unique case is using intake forms for infant patients. Infant forms ask very specific questions because the answers to these questions may influence infant care. In general, they ask about things that a parent or guardian may not think to mention.

Because your practice may also have unique needs, you should use forms that help with HIPAA compliance and can be easily customized. This will be helpful especially when creating more specialized forms, such as baby massage forms. Once you have the various forms you need set up, consider where else you are storing or transmitting electronic PHI. What types of security safeguards do you need to comply with HIPAA online?