What is HIPAA Compliance and

How to Get Started?

This page intentionally left blank.

Introduction

33,500.

This is the number of individuals whose ePHI was exposed due to one HIPAA violation. This one HIPAA violation caused three separate breaches. What was the violation?

MD Anderson failed to encrypt its devices. Three of these devices, a laptop and two thumb drives, were stolen. This seemingly simple breach cost the organization $4.3 million in civil penalties.

Could your practice afford to pay even $50,000 for a single violation? This scenario is more likely than you may realize.

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 HIPAA-compliant forms.

Why is HIPAA compliance crucial?

—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. It's constantly changing.

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

As mentioned earlier, 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

Even a photo of a patient sitting in your waiting room is protected health information because it connects the patient to your practice.

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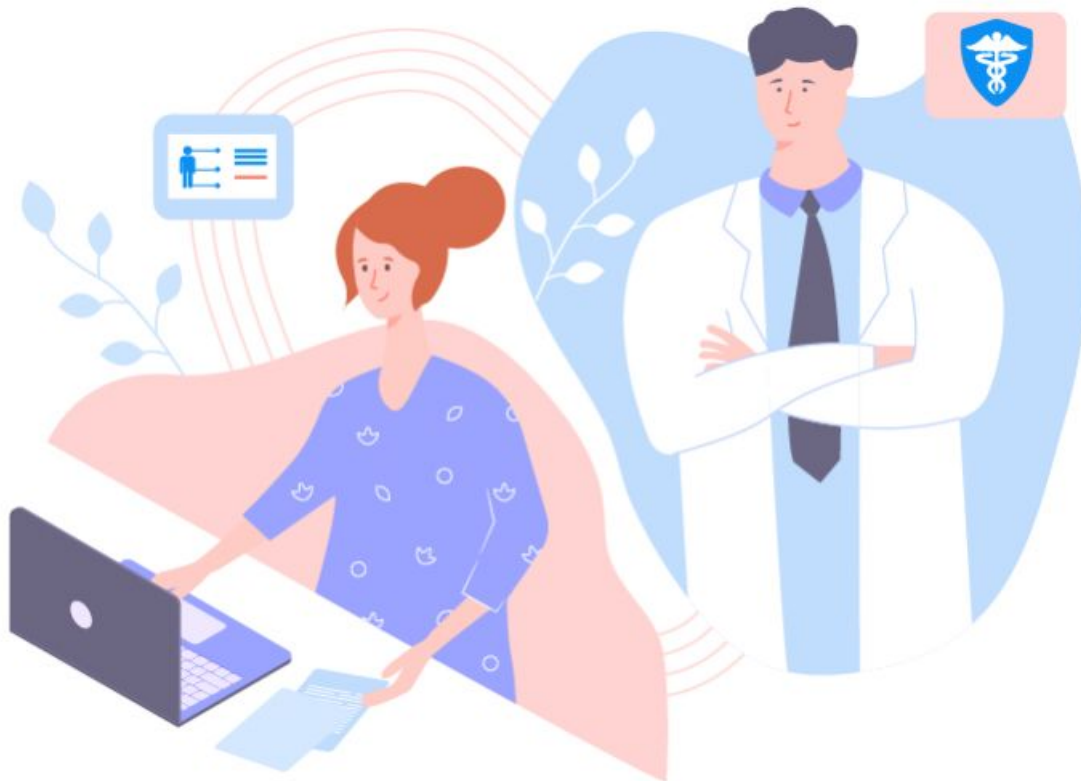
The Gale Encyclopedia of Surgery and Medical Tests defines confidentiality as "the right of an individual to have personal, identifiable medical information kept private. Such information should be available only to the physician of record and other health care and insurance personnel as necessary."

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.

In 2013, a pharmacist at a national pharmacy chain accessed the health records of her husband's ex-girlfriend, who lived more than 150 miles away. The pharmacist discovered that the ex-girlfriend was taking medication for a sexually transmitted disease. After the pharmacist confronted her husband, he contacted his former girlfriend.

Anyone would feel embarrassed when such private medical information is spread around. Because the patient's right to confidentiality had been breached, she sued the pharmacy and won.

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.

A nurse at a mid-sized clinic accessed the health information of a driver who was suing her husband for personal injury after a car accident. After viewing the medical records, the nurse gave the information to her husband's lawyer. She believed the lawyer could use the information to get the lawsuit dropped. However, she violated the driver's rights.

The nurse now faces up to $250,000 in fines and 10 years in prison for attempting to profit off her access to medical records.

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.

One recent scam has seen people using the opioid crisis for personal financial gain. They target individuals addicted to painkillers with expensive cures for opioid addiction. The U.S. Food and Drug Administration is working with the Federal Trade Commission to prevent these individuals from misleading vulnerable consumers and potentially delaying lifesaving addiction treatments.

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.

For example, patients may feel violated if staff members discuss patient information while other patients are nearby. If your practice has a data breach, your patients feel less secure.

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.

Patient confidentiality laws you need to know about

"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 lesser-known patient confidentiality related HIPAA security rules you need to know:

- **Directory information rule.** If a patient is admitted to a facility or an emergency room, you can relay the patient's location and general health status to a person who calls and asks about that patient by name. However, it's unacceptable to share any information with a caller if the patient just has a routine exam.

- **Treating physician rule.** If a person calls your office claiming to be treating your patient, no signed forms are needed. However, you're only required to share information that you deem relevant to the other physician's treatment of your patient. That leaves a little bit of a gray area. What exactly is considered relevant is up to your professional judgment.

- **Social media rule.** Many practices are so afraid of HIPAA violations that they overlook how to share health information legally on social media. Using health information, such as real patient experiences, on social media can be a very effective marketing tool for your practice. To use it, you'll need a signed PHI release form from the patient that includes what information you will use, how you will use it, and for how long.

- **Business Associate Agreement (BAA) rule.** A business associate is any third party that you grant access to protected health information for business purposes. Business associate agreements are legal contracts that define how your business associate maintains HIPAA compliance. If you authorize access to ePHI to anyone outside of your organization, you must have a signed BAA from that person.

- **Departing doctor rule.** Medical professionals who leave a practice may think their patient records go with them. In a multi-physician practice, that's not always true. Protected health information belongs to the covered entity, the practice. If you choose to transfer the PHI to the departing physician, you'll need to get a signed records custodian agreement from each patient and a BAA from the departing doctor.

Failure to follow these rules can land your practice in very hot water.

Consider what happened at Michigan State University. Recently, the university faced intense scrutiny and potential fines for not reporting the removal of patient records from a university clinic. Although staff knew the records had been taken, they didn't notify the patients or get their consent.

Why didn't they think this was a reportable privacy breach? Because they forgot about the departing doctor rule.

The records were allegedly given to Larry Nassar, who had previously treated all of the patients. As you may recall, Larry Nassar is the physician who was convicted of abusing gymnasts in the USA Gymnastics program while providing them with medical care.

The removal of records without proper authorization was a violation of HIPAA law. If staff had remembered that a departing doctor doesn't necessarily have a right to patient files, they might have taken the event more seriously.

To report violations promptly, your staff needs to know what actions are considered HIPAA violations.

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 HIPAA-compliant 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.

For example, an orthopedic practice in North Carolina found themselves in the hot seat with the Office for Civil Rights when they hired a vendor to convert their X-rays to digital media. They worked with a reputable company that managed the X-rays in a professional manner. But the practice made one important mistake. They didn't have the conversion company sign a business associate agreement.

This oversight cost them $750,000 in penalties.

That's right. Penalties for violating HIPAA law can cost you dearly.

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.

Smaller practices may think they're virtually invisible compared to huge health systems and will be overlooked. If you think that way, think again. Private practices like yours are the most scrutinized for this very reason. In reality, the OCR often targets small private practices to set an example and show that no one is immune.

- A <u>12-physician dermatology practice</u> lost a flash drive carrying protected health information. The OCR fined the practice $150,000.

- A <u>five-physician cardiology group</u> had to pay $100,000 for posting patient appointments on an online booking system that allowed other patients to see the names of patients who had already booked appointments.

- A <u>physical therapy provider</u> was charged with failing to reasonably safeguard PHI and impermissibly disclosing PHI without authorization. The provider agreed to a settlement payment of $25,000.

How many records have you turned over to Microsoft, Google, or an even less well-known company without a BAA? Taking a serious look at this could help you uncover and mitigate your risk.

Criminal penalties

The person who directly commits a violation can be held criminally liable under HIPAA rules. Criminal penalties are typically reserved for people who knowingly, and possibly defiantly, commit or attempt to cover up HIPAA violations.

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.

Think doing hard time is excessive for a HIPAA violation? Consider some notable violations that earned individuals time in prison.

Revenge, interrupted

In 2010, the first-ever prosecution for a HIPAA violation happened after a 2003 incident. A researcher fired from UCLA Medical Center wanted to get back at his former employers. He took advantage of his access to medical records to view information about managerial staff, likely searching for embarrassing medical information.

He also accessed the records of numerous celebrities, including Drew Barrymore, Leonardo DiCaprio, and Tom Hanks. He may have hoped to profit from selling something to the tabloids. Because the system was monitored, the breach was identified before any harm could be done.

He got four months and was fined $2,000. If he had shared any of that information, the penalty would have been much higher.

Almost rich

A 30-year-old man was sentenced to 18 months in prison for collecting protected health information at the Texas hospital where he worked. He intended to sell the information on the black market. Many considered his sentence light. If he had sold any of the data, he could have gotten 10 years.

Addiction and desperation

A respiratory therapist accessed more than 500 patient records over 10 months. Her goal was to obtain intravenous drugs under the pretense that the patients needed them. However, the drugs were shipped to the practice addressed to her. The prosecution argued that she intended to use the drugs to feed her own addiction.

She faces up to one year in prison, and the hospital where she worked could face additional penalties for not catching the violation sooner.

How to identify your risk level

"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by [your practice]."

—U.S. Department of Health and Human Services

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.

Leave no stone unturned.

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.

A few codes on a bill may not seem like much, but they're protected health information. Sharing them without having the proper forms signed is a sanctionable HIPAA violation. Make sure to look everywhere for PHI during your risk assessment.

What external entities have access to your PHI?

External entities include vendors and subcontractors. They can even include basic computer programs like Microsoft Word if someone uses it to type up patient cases.

When using any software to manage protected health information, remember to get a business associate agreement. A verbal agreement isn't enough. Neither is a statement on a company's website stating that they're HIPAA compliant. Always have a signed BAA before using a business associate's product.

For example, JotForm allows you to create custom, electronic forms that are fully HIPAA compliant. Their forms support secure collection of patient data and signatures online. When they sign a business associate agreement with your practice, they assume full responsibility for keeping that protected health information safe.

What risks does PHI face?

The risks to protected health information come from humans, malware, natural disasters, or even a major power outage.

In 2017, the ransomware aptly named "WannaCry" brought one of the world's largest healthcare systems to its knees. Hackers used the ransomware to lock down the United Kingdom's National Health System. They demanded payment in exchange for decrypting patient records. At the same time, several U.S.-based health systems were hit. In most cases, the affected medical centers chose to pay rather than lose their patient records forever.

It was a hard lesson.

HIPAA requires that you make patient records available to patients within a reasonable amount of time. If your patient records are locked down by ransomware, how would you fulfill your HIPAA obligations? Planning for these types of scenarios is part of your risk assessment.

While evaluating your risk levels, you'll undoubtedly find new risks. You may even uncover some violations. Never push what you find under the rug, and don't wait to resolve it. Address any risks or violations immediately to avoid more violations and even bigger penalties.

Once you've found the risks to HIPAA compliance, train your staff on how to stay HIPAA compliant.

HIPAA training essentials

HIPAA states that <u>training should be provided</u> "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.
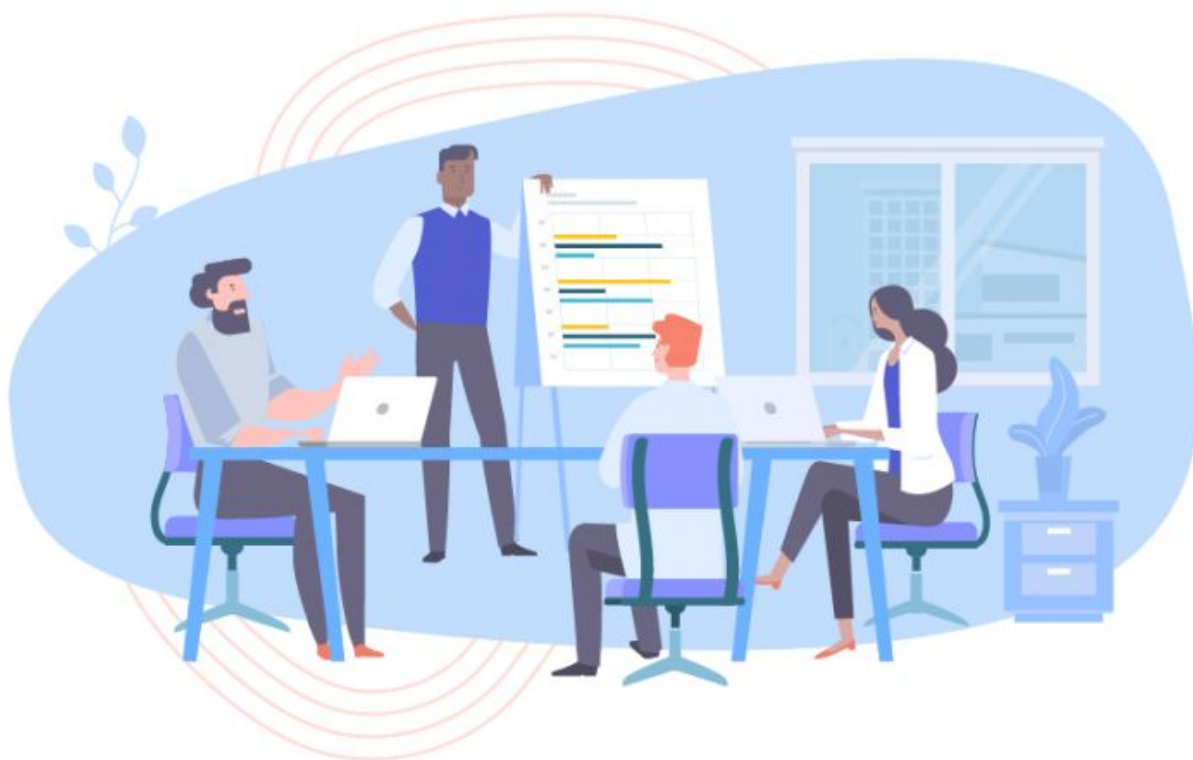
Those who need training could be in a variety of departments, including

- 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.

Communicate the gravity of the law to them. Then, have someone follow up with them to make sure they're following the rules.

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?

Stipulate any disciplinary measures for violating HIPAA, and follow through with them. Your practice can't afford to keep an employee who doesn't "get it." When you show how serious you are about HIPAA training and enforcement, your employees will know they can't be lackadaisical about compliance.

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.

If any of the new guidance has a significant impact on your practice, don't wait until the next scheduled training to inform staff. Do it immediately.

One new technology that has had a direct impact on HIPAA training is social media. How can your employees use social media and still be HIPAA compliant?

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.

Make sure your employees know what can't be shared on social media:

- Never discuss a patient even if you don't use their name. Someone who knows them may put two and two together.

- Never discuss health information through social media messaging or comments even if the patient initiates it.

- Never share pictures of patients in or around your practice without written consent. Use a medical information release form designed specifically for social media.

- Always get a signed medical information release form from the patient before sharing their stories on social media.

Verbal consent isn't enough. Be sure to get patient consent in writing using the proper form. A release form is useful for social media, but what other HIPAA forms do you need in your practice?

What are the main types of HIPAA forms?

In the medical industry, the maxim "not documented, not done" highlights the importance of keeping accurate medical records. As you can imagine, HIPAA has a number of requirements regarding documentation. Always keep HIPAA-compliant forms pertinent to your practice on hand to use with your patients.
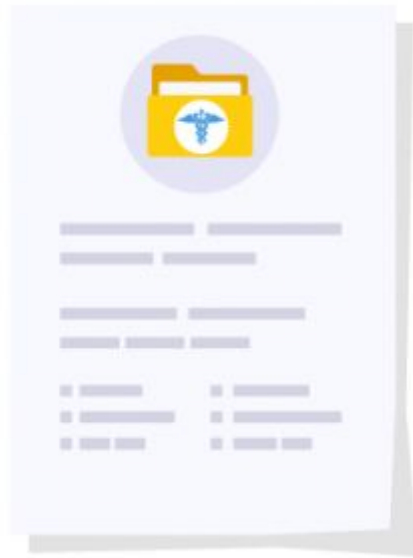
Receipt of privacy agreement form

This form documents that the patient acknowledges receiving a copy of your privacy agreement, which states how you comply with HIPAA to protect patient information. A privacy agreement also explains that a patient has the right to request and receive their medical records.
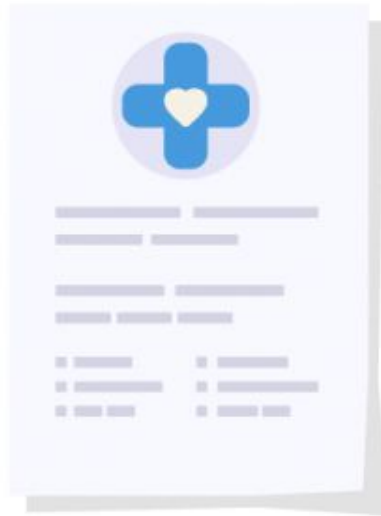
HIPAA medical release form

You'll need to complete this form when sharing medical information with someone other than the
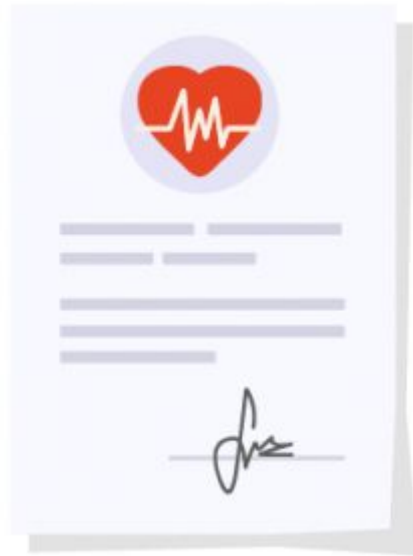
- Patient

- Patient's legal representative

- Treating physician

- Health insurance company

- Pharmacy

Remember that this information can only be shared on a need-to-know basis to protect the patient's confidentiality.

You'll also need a signed release form from the patient when

- Sharing PHI with a university for research or educational purposes

- Sharing records with the patient's attorney for a personal injury lawsuit

- Transferring records to a departing physician who will continue attending the patient

- Using a patient's personal recovery story as part of a marketing campaign

While the patient must give their consent to share their protected health information, you may need additional forms depending on the circumstances.

Records custodian agreement

A records custodian agreement is the form that a departing physician signs when taking patient records to a new practice. It transfers the responsibility for the storage and use of medical records from the covered entity to the departing provider.
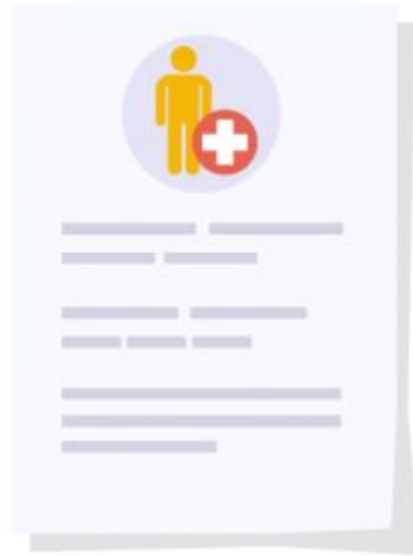
Patient intake form

Patient intake forms gather the basic information that you need to know about new patients. Well-designed electronic patient intake forms can significantly enhance the patient's experience. They also streamline the intake process.

Patients appreciate being able to easily and securely fill out the encrypted form at home or on their smartphone before their appointment. Plus, your practice benefits by having all of the patient's information before their next appointment.

By using a patient intake form, you'll be able to

- Understand the reason for their visit

- Verify their insurance

- Review and update office notes

- Better assess appointment length
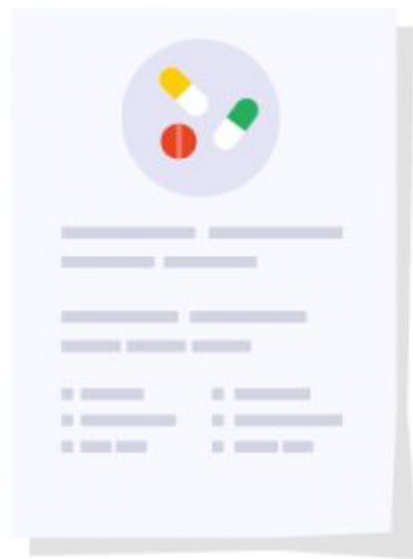
Medication and prescription refill forms

These electronic "prescription pads" make it easy to send prescriptions to the pharmacy. Electronic prescription forms put an end to deciphering messy handwriting, photocopying, filing paper scripts, waiting on hold for the pharmacist, and asking sick patients to wait at the pharmacy. They speed up the process so prescriptions are ready when the patient arrives.

Additional benefits of this form are updating existing prescriptions electronically and having a permanent copy of the form in the patient's electronic file.

Payment request form

Over half of bills are now paid online. If you're only accepting traditional payment methods or mailing out monthly bills, you could be contributing to nonpayment and increased overhead. After all, time and postage aren't free.

By sending payment request forms to patients through HIPAA-compliant email, you make it easier for patients to pay their bills. You also reduce your administrative workload. Using these forms in conjunction with common payment processors, like PayPal, Stripe, or Square, makes for a powerful combination.
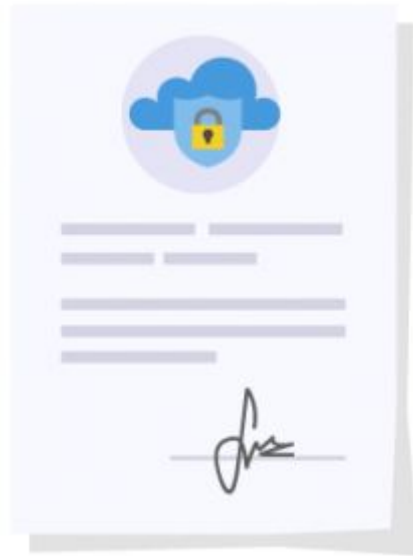
Business associate agreement

The business associate agreement is a written agreement between you and an individual or entity outside your practice. A business associate could include any software and cloud services that are receiving, transmitting, processing, or storing protected health information. If you use a number of third-party apps that integrate with your software, each app must sign a business associate agreement.

When an entity signs a BAA, they acknowledge their responsibility to keep PHI safe. They also confirm that they have systems in place to comply with HIPAA regulations. Without a signed BAA form, your practice is responsible for any mishandling of PHI that happens on the third party's watch.

As you've seen, there are HIPAA-compliant forms for all areas of your business. Now that you know a little about each one, let's take a closer look at the form that starts your HIPAA responsibility.

The first step in HIPAA compliance: Intake forms
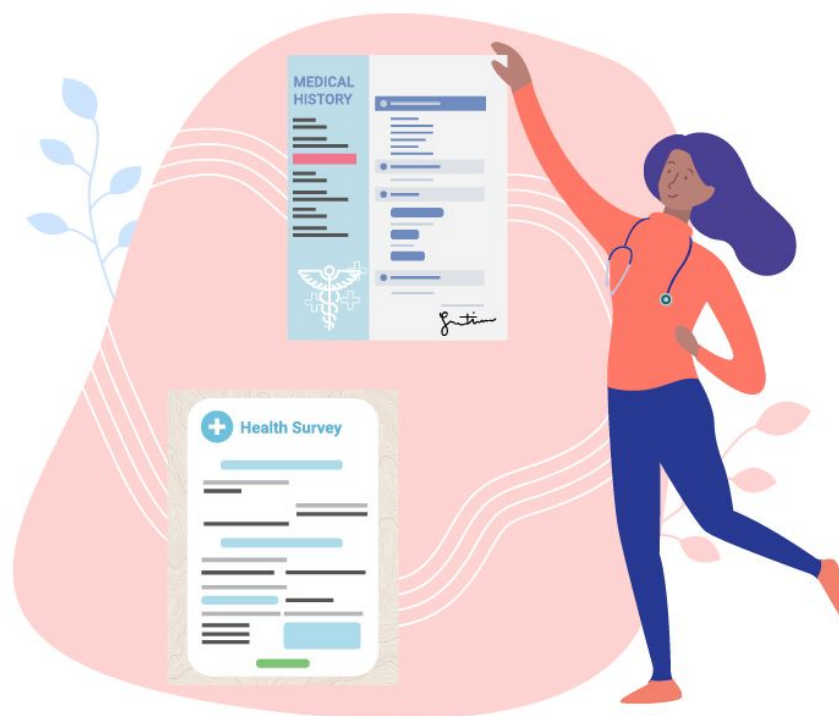
Intake forms are the cornerstone of protected health information in a practice. The vital information that they contain enables you to better treat your patients. But you are also responsible for protecting that information.

In the modern era of HIPAA, paper forms simply pose too great a risk to compliance. Why? Protected health information on papers forms can be easily exposed:

- While patients fill out paper forms in waiting rooms, others can look over their shoulders.

- Forms may stay on a staff member's desk for days before being manually entered into a computer system or filed.

- Forms may unwittingly be thrown into waste bins rather than shredders.

- Forms may wait in a closet to be shredded because, really, who has time to shred papers in a busy practice?

Electronic forms, on the other hand

- **Cut wait times.** Patients can easily fill them out on their home computer or smartphone before their appointment.

- **Eliminate inefficiencies.** If a patient is late to their appointment, you won't need to wait another 10 minutes for them to complete forms. They'll already have finished them before arriving. You also won't have to transfer written information from a handwritten form into a computer.

- **Reduce booking gaps and overbooking.** Patients will be more aware of their appointments and less likely to miss them when they fill out forms in advance. Intake forms can also be reviewed beforehand to better judge how long certain visits may take.

- **Project a modern image.** Many patients judge a practice's level of care on the intake process. Intake forms shouldn't be an afterthought. Having a streamlined electronic intake process lets your patients know that your practice is modern, organized, and efficient.

- **Streamline appointments.** Not everyone enjoys filling out forms on the internet, but most patients will appreciate how electronic forms streamline their appointments.

- **Are flexible.** Not everyone has internet access, but that doesn't mean you can't or shouldn't use electronic forms. Allow these patients to fill out their forms on a tablet when they arrive.

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 stay HIPAA compliant.

- **Randomized URLs** like https://www.jotform.com/uploads/user/63043229924960/353747904850626197432/JotForm-icon.png make it impossible for a hacker to guess at file names. This adds an extra layer of security by making files harder to find in the first place.

- **An SSL certificate** means that all patient data is transmitted securely, fully encrypted, and impossible to hack. JotForm uses the same advanced technology that major banks use to prevent financial information theft.

- **Unique logins** for patient and office staff provide extra security by discouraging account sharing.

Technical safeguards are essential to keeping intake forms and protected health information safe. But without human cooperation, your forms will still be vulnerable. Technology and your team must come together to maintain security throughout the practice.

Consider four ways you can work on the human firewall that will keep patient intake forms and all PHI safe:

- **Complete a thorough risk assessment.** Do you remember what happened in the WannaCry attack? You don't want to be crying over HIPAA penalties because you failed to do a complete risk assessment. Make this a top priority in becoming HIPAA compliant.

- **Train your staff on proper security protocol.** Employees should always lock their computers when they step away from the desk. They should also create strong passwords that they don't use anywhere else. And, remind them to never click on suspicious links in emails.

- **Update software promptly.** When your computer sends you an update notification, this often means that a vulnerability has been discovered. The software company has patched it promptly, but you must install that patch. Every hour you wait, you remain vulnerable to a known threat. Updating software is part of managing risks promptly.

- **Lead by example.** Demonstrate that you follow the same rules you've put in place for other staff members. All members of your staff must be HIPAA compliant, so leaders need to show that they are dedicated to HIPAA compliance.

Every practice needs an effective patient intake process, but sometimes there are unique situations that call for special attention. Providing massage therapy and attending to infants are two examples of these unique intake situations. Let's look at both.

How to use massage intake forms

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. They are useful to

1. **Make a great first impression.** Massage is a notoriously competitive business, and many clients pay for massages to get pampered. Electronic massage intake forms offer this discerning type of client the seamless experience that leads them to schedule their next appointment.

2. **Get to know your clients.** Massage intake forms are a great way to effortlessly start a conversation with a new client. You can learn more about why the patient decided to come in. Then, use what you learn to tailor recommendations for services and packages to the patient.

3. **Market to repeat clients.** Massage intake forms are a non-intimidating way to get someone's email. Once you have them on your mailing list, you can send tips, offers, and other marketing by email. As long as you send marketing emails at a reasonable frequency, stay relevant, and obey all email marketing laws, they'll usually stay subscribed and visit you more often.

How to use intake forms for infants

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, for example

- Does the baby eat anything other than breast milk?

- Does the child have known food allergies?

- Is your child on a special diet?

- What does your baby use to drink?

- What frightens your child?

In addition to specific questions, an infant form will include a request for parental or guardian consent to treat the child.

Because your practice may also have unique needs, you should use HIPAA-compliant forms that 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?

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.

Think about it. Where are you safest on a typical day? At home, at work, or during your commute? Statistically speaking, you're much more likely to have an accident in transit between destinations. In the same way, information is most vulnerable when it's in movement.

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.

What are the requirements for HIPAA-compliant servers?

Any server your practice uses must be HIPAA compliant. 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.

A HIPAA-compliant server must safeguard the integrity, confidentiality, and accessibility of health information. Be aware that the Department of Health and Human Services doesn't recognize any organization as a certifying body of HIPAA-compliant servers. So do your homework to confirm that a server is HIPAA compliant. Then, get a BAA signed before using it. These steps are essential to safeguarding your patients and your practice.

For any server to be HIPAA compliant, 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

Let's look at some of the top HIPAA-compliant software service providers.

Best HIPAA-compliant email providers

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 six of the best HIPAA-compliant email service providers:

- **Aspida Mail** allows simple yet secure email migration.

- **NeoCertified** provides easy access through a secure portal.

- **Paubox** turns your existing email into HIPAA-compliant email. It works with Gmail and other popular email services.

- **Protected Trust** turns Outlook and other Windows applications into HIPAA-compliant software.

- **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 HIPAA-compliant hosting.

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

Best HIPAA-compliant cloud storage and file sharing services

"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.

However, several companies that offer services to the average consumer also have paid services that are HIPAA compliant. Getting secure storage requires upgrading to these more advanced versions of cloud and file-sharing software. Because they will store protected health information, always get a signed BAA before allowing staff to use any cloud drive.

Here are five of the top HIPAA-compliant cloud storage and file-sharing solutions for your practice:

- **Box** provides seamless integration into existing healthcare systems. Although it's a newcomer to cloud storage, it's quickly claiming market share because of its flawless user experience.

- **Carbonite** offers built-in, multilocation backup to ensure that medical records are always accessible, even during a disaster. It is a more costly option, but it has been in the cloud business since 2005 and is one of the most respected brands in the industry.

- **Dropbox** is HITECH- and HIPAA-certified by an independent certification body. It offers up to five accounts for a low monthly price and can be integrated with many helpful third-party applications, like JotForm.

- **Google Drive** easily integrates with Google's online office suite. It also gives you tiered control to limit PHI access to a need-to-know basis.

- **Microsoft OneDrive** has many options for tracking user behavior. Although it's more expensive than other compliance options, it offers greater control over who can access sensitive data.

After securing your data, next you should consider which HIPAA-compliant software you'll need to use in your practice.

Best HIPAA-compliant software

To run a practice in the 21st century, you 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.

Here are four of the best HIPAA-compliant software programs for practices:

- **Google G Suite** has been HIPAA-compliant certified by an independent certifying body. In addition, it's certified as ISO-27017, which expanded data access controls over previous security standards. Because your employees probably already use Google products, this software is very easy to integrate into your office.

- **Microsoft 365** has obtained HIPAA-compliant certifications from multiple independent organizations. Plus, its software suite includes programs that most people who work in offices already know how to use.

- **UpDox** is a HIPAA-compliant company that built its software specifically for the needs of healthcare practices. It offers advanced features, such as appointment reminder automation. It also has a patient portal so that patients can communicate with medical staff, access test results, and pay bills online.

- **JotForm** provides users with the tools to create, manage, transmit, and store custom HIPAA-compliant forms. This mobile-friendly tool is easy to use and can be embedded in email, websites, and other applications. It allows you to request information and transmit prescriptions to equipment providers and pharmacies electronically. You can effortlessly acquire signatures and accept online payments to provide services and get paid more quickly.

Now that you're using HIPAA-compliant software, what everyday guidelines should you be following to protect health information in your office?

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?

Becoming HIPAA compliant: Where to start

Many people want to know the minimum necessary standard so that they can become HIPAA compliant more quickly. That's really hard to determine because every healthcare practice is different.

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 HIPAA–compliant software** 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 HIPAA-compliant forms 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 HIPAA-compliant form service for your practice, 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.

Remember that even a small practice has an enormous, and potentially overwhelming, responsibility to be HIPAA compliant. Show your concern for securing protected health information by using HIPAA-compliant forms. Integrate them into your existing recordkeeping system. Use them to centralize and automate PHI management.

In this way, you and your team will have to worry about fewer HIPAA protocols. You'll also demonstrate to the Office for Civil Rights that you have trusted systems in place to protect health information. In the event of an investigation, your obvious concern for HIPAA compliance will work in your favor.

To learn more about how you can accomplish this level of HIPAA security, centralization, and automation, get HIPAA-compliant forms from JotForm.