NEXCESS

EBOOK

Eliminate 7 HIPAA risks with one simple decision

Table of contents

Executive summary

This ebook explores seven critical website-related risks that can put healthcare practices in violation of HIPAA regulations, often without their knowledge.

These risks include:

1. The high financial cost of a single breach, which can exceed $1 million in direct and indirect expenses.
2. Elevated penalties for “willful neglect,” when a known issue goes unaddressed.
3. Mandatory public breach disclosures, which can lead to reputational damage regardless of breach size.
4. The misconception that SSL alone equals compliance, when HIPAA requires much more comprehensive safeguards.
5. The use of shared hosting environments, which often lack the necessary controls to protect patient data.
6. The challenges of scaling digital tools without a compliant infrastructure to support them.
7. The burden placed on staff to manage security risks they were never trained to handle.

While each risk poses a serious threat, they all share a common solution: moving your website to a HIPAA-compliant hosting environment with the proper technical, physical, and administrative safeguards in place.

Practices that make this single decision benefit from reduced liability, improved operational efficiency, and stronger patient trust, without the need for a complete digital overhaul. This ebook provides practical guidance for identifying risks, making informed infrastructure choices, and taking immediate steps to align your website with HIPAA standards.

Whether you're a physician-owner, executive director, or practice leader, this guide is designed to help you protect your patients, your reputation, and your bottom line.

Introduction

This ebook is written for leaders and decision-makers at healthcare practices who rely on their websites to connect with patients, but may not realize the hidden risks those websites carry.

This ebook is especially relevant for:

- Physician-owners of small and mid-sized practices
- Executive directors and operations leaders at multi-provider clinics
- Practicing physicians who play a role in digital decision-making
- Website or IT managers responsible for digital infrastructure and compliance

Whether you run a primary care clinic, an urgent care center, a dental or chiropractic office, or a sleep medicine practice, if your website or application collects or transmits patient information—even through something as simple as an appointment request form—you are subject to HIPAA's requirements.

What you'll learn

In the pages ahead, you'll explore seven of the most common and costly HIPAA compliance risks tied to healthcare websites. These include financial exposure, public breach reporting, misconceptions about security, and the challenges of growing your digital capabilities without the right foundation.

But more importantly, you'll see how each risk can be avoided—not through complex technical fixes, but through one clear, proactive decision: moving your website or application to a HIPAA-compliant host.

Why this matters now

Many practices assume their website is “just marketing.” But in today’s healthcare environment, it’s much more than that. Your website is a front door, an intake tool, a communications channel and increasingly, a legal responsibility.

As regulations tighten, technologies evolve, and patient expectations rise, the cost of not addressing these risks grows with each passing month. This ebook is your chance to get ahead of the problem, protect your practice, and make a smart infrastructure decision that sets you up for long-term success.

Risk 1

A single breach can cost over $1 million

Most physician practices don't see their website as a financial risk. But if your site collects patient information—whether through contact forms, appointment requests, or if you allow patients to upload intake documents—it's handling protected health information (PHI). If that data isn't secured properly, the consequences can be devastating. The same is true with other applications like your EHR, practice management, or patient portal solutions.

According to industry data, the average cost of a healthcare data breach is around $10 million.

Here's where the costs stack up:

- Regulatory fines from the Office for Civil Rights (OCR)—the entity that enforces HIPAA—can reach $50,000 per violation, and go higher for repeated or willful neglect
- Legal fees and settlements may follow if patients pursue legal remedies, especially if sensitive data like a diagnosis or insurance details were exposed
- Forensic audits and system recovery become necessary, often involving third-party investigators and consultants
- And then there's the cost of lost trust and brand reputation; referral networks may hesitate to send new business your way and existing patients may look for care elsewhere

The most common misstep? Thinking the risk only applies to big hospital systems or EHR vendors. Smaller practices often face greater exposure because they don't have full-time IT security personnel and don't realize their website is a HIPAA compliance touchpoint until it's too late.

The good news:

This isn't a warning meant to scare. It's meant to clarify. Website-related risks are entirely preventable if you know where to look. Ensuring that your site and other applications are hosted in a HIPAA compliant environment, with secure backups, access controls, encryption, and a signed business associate agreement (BAA) closes the door on one of the most overlooked vulnerabilities in private practice today.

PRO TIP

One small mistake can lead to seven-figure consequences.

Risk 2

Fines increase if you knew ie, “willful neglect”

In the eyes of regulators, not knowing is one thing. Knowing and not acting is something else altogether, and it’s treated much more seriously under HIPAA.

If your practice collects patient information through your website, you’re considered a covered entity under HIPAA. That means you're responsible for ensuring that protected health information (PHI) is handled securely, even if the tools you're using—like your web forms, hosting provider, or contact widgets—were set up by a third party.

This is where the concept of “willful neglect” comes into play. If the Office for Civil Rights (OCR) determines that a practice knew about a HIPAA requirement and failed to comply, the penalties move into a much higher tier. We’re talking:

- Minimum fines of $10,000 per violation
- Up to $1.5 million per calendar year, per type of violation
- Potential audits and formal corrective action plans

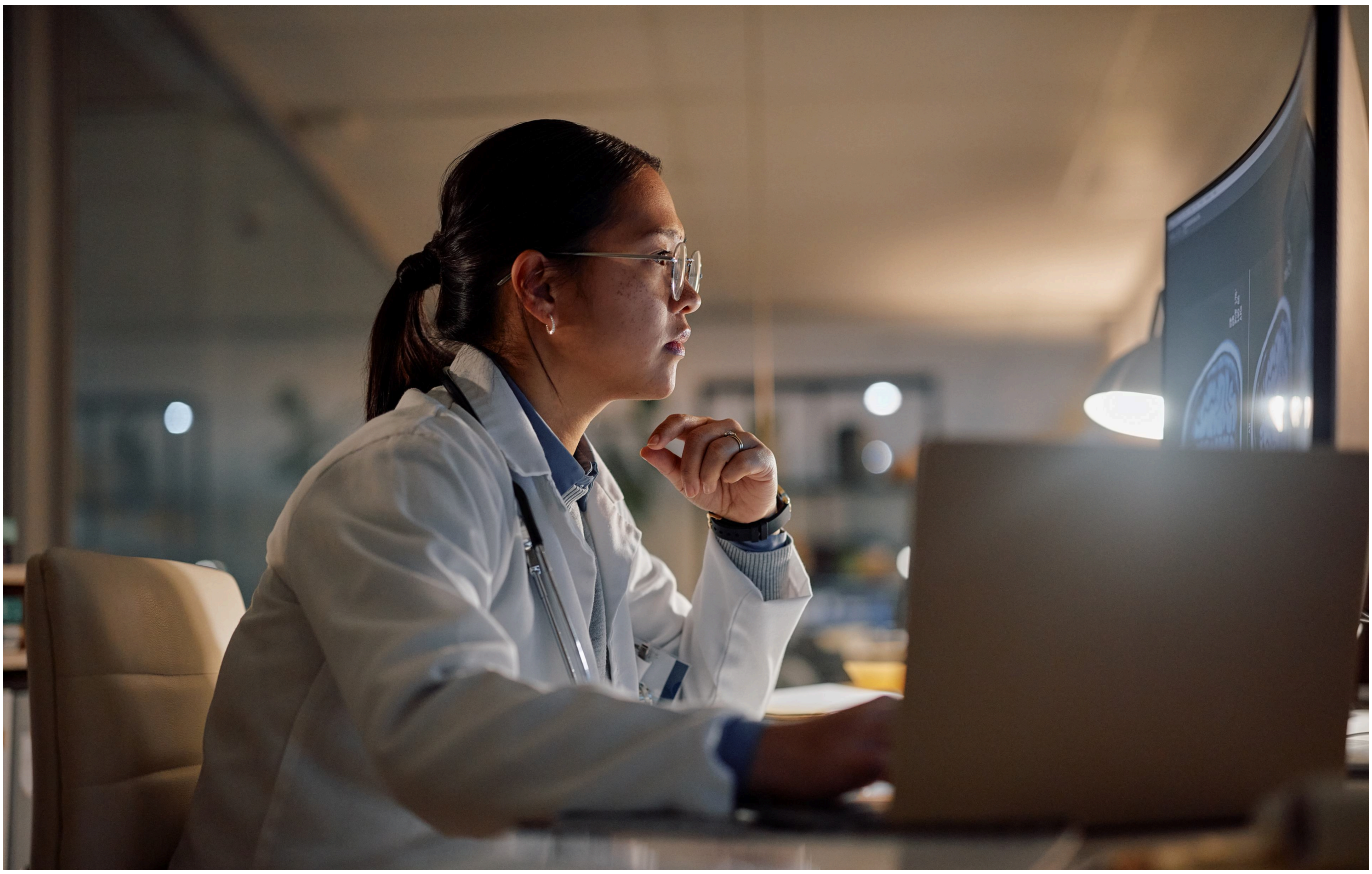
And it doesn't take a massive breach to trigger scrutiny. An anonymous complaint, a report of a misrouted message, or a patient data concern can all prompt an investigation. Once that happens, if it's discovered that your practice never secured a business associate agreement (BAA) with your website host, or didn't encrypt sensitive transmissions, it could result in a penalty. Even small gaps can turn into large liabilities.

What qualifies as "knowing"? Often, it’s as simple as having had the issue flagged by a staff member or vendor and choosing not to correct it in a timely manner. In other words, once you’re aware there’s a risk, you’re on the hook for fixing it.

The good news:

You don’t need to be a security expert to meet your obligations. What matters is that you take reasonable steps to protect PHI. This includes choosing a hosting provider who understands HIPAA, is willing to walk you through different compliance options, is willing to sign a BAA, and helps you meet privacy regulations as well as patient privacy expectations proactively. This one decision can eliminate the risk of willful neglect altogether—and spare your practice from the most severe fines down the road.

Knowing there’s a problem and doing nothing carries the highest penalty.



Risk 3

Breaches go public whether you want them to or not

When it comes to healthcare data, it is impossible to keep a breach quiet.

Any data breach must be reported to the U.S. Department of Health and Human Services (HHS).

Breaches affecting fewer than 500 individuals must be reported to the Secretary before Oct. 31 of the year the breach is discovered. Breaches affecting 500+ individuals must be reported to the Secretary no later than 60 calendar days from the discovery of the breach.

These larger breaches are published on what is commonly referred to as the HIPAA Wall of Shame—a public database accessible to anyone, including patients, news outlets, and your immediate community.

In addition to the HHS, you may also be required to:

- Notify each affected individual directly
- Inform local media in your region
- Provide a public statement or press release about the incident

That means that even a small website oversight, like an insecure contact form or a misconfigured upload tool, could end up being a media headline. Even if the breach was relatively small, the perception it creates can be disproportionately damaging.

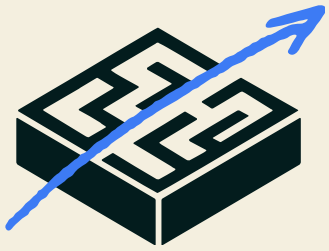
Here's why this matters to your practice:

- Reputation loss: Once patients hear that their health data may have been exposed, trust takes a hit, and it's hard to recover
- Referral strain: Larger providers in your network may hesitate to send patients to you if your data practices are in question
- Digital footprint: Breach reports and media stories don't disappear—a constant challenge for your practice to overcome

Knowing the risks allows you to be prepared. It's important that practices see their websites as more than just a marketing tool. It's a gateway to your practice for patients and as such, it's a key part of your privacy infrastructure. Because of the potential consequences, your website deserves your attention.

The good news

Hosting your site and other applications in a HIPAA compliant environment with proper safeguards dramatically lowers your risk of a breach and positions your practice as one that takes patient privacy seriously. It's a smart step, not just for compliance now, but for protecting your name and your future.



Breach disclosure isn't optional. Neither is the fallout.

Risk 4

SSL isn't HIPAA compliance

If your website has a padlock icon in the browser bar, that's a good start. But it's not enough. SSL (Secure Sockets Layer) only protects data in transit. It doesn't make your website HIPAA compliant.

This is one of the most common and costly misunderstandings we see among physician practices and specialty clinics. A website secured with SSL looks compliant from the outside, but being HIPAA compliant means securing how patient information is collected, stored, accessed, and backed up.

Let's break it down

SSL helps:

- Encrypt the connection between a visitor's browser and your website
- Prevent "eavesdropping" when someone fills out a form or submits a message

But HIPAA requires:

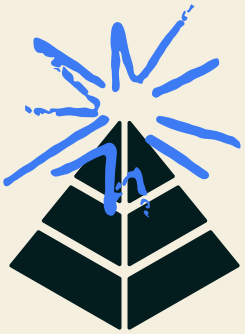
- Encrypted backups of any data collected through the site
- Access controls that limit who can view or download that data
- Audit logs to track who accessed what and when
- A signed business associate agreement (BAA) from any vendor that handles protected health information (PHI), including your web host

So, if your hosting provider doesn't provide a signed BAA, or if data collected on your website or other applications you're using isn't stored in an encrypted and secure manner, your practice may be out of compliance—even if the site has SSL.

The result? A false sense of security. And in a HIPAA audit or breach scenario, that illusion can quickly become a liability.

The good news

You don't need to know every technical detail of HIPAA to meet the standard. But you need to work with partners who do. Hosting your website and applications with patient data with a provider that understands healthcare requirements and has the necessary privacy infrastructure means you will avoid the honey trap of partial protection with just SSL.



Full protection means SSL encryption and HIPAA compliance.

Risk 5

Hosting on shared infrastructure may violate HIPAA

Most commercial websites are hosted on shared infrastructure. In this setup, your site resides on the same server as dozens, sometimes hundreds, of others. It's fast and affordable, but when it comes to handling sensitive health information, shared hosting may not be HIPAA compliant.

Here's why

HIPAA requires technical, physical, and administrative safeguards for protected health information (PHI). That includes controlling who can access the systems where PHI is stored. With shared hosting, you don't have that level of control.

In many shared environments:

- You have no visibility into who else is using the server
- Server resources are pooled, meaning a vulnerability in one site could affect another
- Isolation is minimal, increasing the risk of unauthorized access
- The hosting provider may not sign a business associate agreement (BAA) for shared environments—a non-negotiable HIPAA requirement

Even if your own site is well-designed, the server it sits on could be the weak link. If another customer's website on the same server gets compromised, the damage may extend to your environment and your patients.

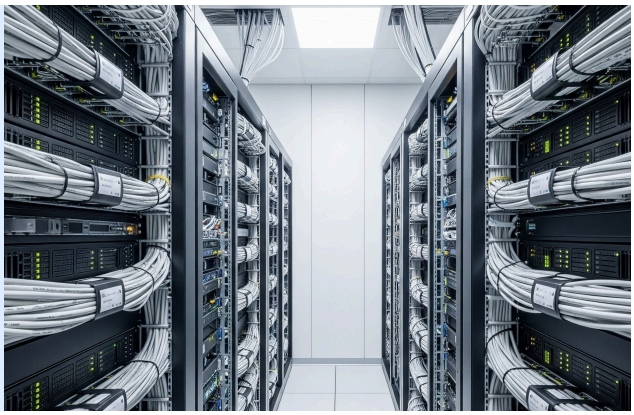
In addition, HIPAA requires that any technicians who work on a server maintain detailed logs of their activity, including what they accessed, when, and why. These individuals must also be covered under a BAA, which typically includes specialized privacy training. In a shared-server environment, this level of documentation and oversight can sometimes be inconsistent or lacking.

That's not to say every shared server is dangerous. But unless it's explicitly configured to meet HIPAA standards, and your provider has agreed in writing (via a BAA) to take on responsibility, shared hosting should be considered high-risk for any healthcare practice.

The good news

You don't have to overhaul your entire site to fix this. Moving to a dedicated or HIPAA-configured hosting environment is a straightforward process, especially when managed by a provider that understands both the technical setup and the compliance requirements. It's one change that immediately reduces your exposure. It also shows your staff and referral partners that you take data security seriously.

You can't protect PHI on a server you don't control.



Risk 6

Growth without a secure foundation

Healthcare changes quickly. From online scheduling and digital intake forms to virtual care and AI-powered tools, new technologies are reshaping how practices engage with patients. But none of these tools can be safely deployed if your website and application hosting infrastructure aren't secure and compliant from the start.

If your website isn't built on a HIPAA-compliant foundation, every new feature, form, portal, or app you add will introduce more risk. As you grow, these risks amplify one another until you have a complex privacy mess to untangle.

We see this especially in:

- Multi-site practices trying to unify digital experiences
- Urgent care centers adding online check-ins
- Small clinics launching telehealth services or digital marketing campaigns

The problem? Scaling on top of a non-compliant environment is like building a second story on a cracked foundation. Eventually, something breaks.

HIPAA doesn't just apply when you get "big enough." It applies from the moment you collect, store, or transmit protected health information (PHI). If you're planning to grow, or already are, you need a compliant foundation now.

The good news

You don’t need to rebuild everything from scratch. By choosing a HIPAA-compliant hosting provider now, you create a safe, scalable platform for whatever comes next—whether it’s digital forms, secure messaging, or new tools that haven't even hit the market yet. It’s a future-proofing decision that protects both your growth and your patients.

The time to build a compliant foundation is before you grow.

Risk 7

You don’t want your staff dealing with privacy and security issues

Your clinical and administrative teams are hired to care for patients and keep your practice running smoothly. They are not there to monitor server logs, configure encryption, or troubleshoot security gaps in your website.

Yet that’s exactly what happens when you rely on general-purpose web hosting that doesn’t meet HIPAA standards. Without the right infrastructure in place, the burden of privacy and security shifts to your staff, whether they’re trained for it or not.

We’ve seen it before:

- Staff selecting and using an application hosted on a non-HIPAA compliant platform
- A marketing manager unsure how to store website form submissions safely
- Practice managers collecting payments through secure, but not HIPAA compliant solutions
- Using a patient portal that’s not secure and compliant

This isn’t negligence—it’s misalignment. These are smart, capable people doing their best with the tools they’ve been given. But if the website platform doesn’t handle compliance properly, it’s unfair and unsafe to expect your staff to “fill the gaps.”

HIPAA violations of this type often stem from workflow issues or uninformed decisions, not malicious intent. You’re at higher risk the more manual workarounds you have.

The good news

The simplest way to take this pressure off your staff is to make sure your website itself is secure and compliant by default. When your hosting environment includes encryption, access controls, backups, and a signed BAA, your team can focus on what they do best—without worrying about what's happening behind the scenes

Let your staff focus on patients—not patching privacy risks.

Conclusion

Across all seven risks we've explored, one truth stands out: your website may be more tightly linked to your HIPAA compliance and your financial health than you previously realized.

These are not hypothetical risks, and they could be present in your practice:

- A contact form that lacks encryption
- A server shared with hundreds of unrelated sites
- A hosting provider that won't sign a BAA, leaving you legally exposed
- EHR, patient portal, or practice management hosted in a non-HIPAA compliant way
- Patient messages stored without proper safeguards or storage controls

And the cost isn't just financial. The ripple effects of a HIPAA violation will erode patient trust, damage your brand, and distract your staff from what matters most: delivering excellent care.

More frustrating is that many practices believe they're covered, simply because their site uses SSL, or because it "wasn't built to collect PHI." But intent doesn't equal compliance. Ultimately, you, as the covered entity, have a responsibility for the information you collect.

The good news: you don't need to overhaul everything. You just need to start with the right foundation.

Moving your site to a HIPAA compliant hosting environment takes the weight off your internal team. It closes gaps that may not be visible from the outside. And it gives you peace of mind that your site is protected not only today, but as your technology needs grow tomorrow.

At Nexcess, we don't just offer compliant infrastructure. We help practices like yours understand what compliance looks like, and how to maintain it in a way that's practical, scalable, and aligned with patient care.

This isn't about doing more. It's about reducing risk.

Next steps

Not sure if your current host is compliant?

Use our HIPAA compliance checklist to review the essential questions every healthcare website owner should ask.

Want a second opinion?

Our HIPAA hosting specialists are available to review your current setup and flag potential risks—no pressure, no jargon.

Already considering a change?

Nexcess offers HIPAA compliant hosting with a signed BAA, encrypted backups, secure infrastructure, and seamless migration support.

Start with one decision

Eliminate the risks. Reclaim your peace of mind. And let your website support your practice, not put it at risk.

About Nexcess

Nexcess is the global specialty cloud partner for mission-critical workloads, backing over 185,000 customers across a global footprint of 100,000 servers. Built for leaders who want their teams focused on execution rather than fighting complex environments, we filter cloud complexity to turn technical hurdles into opportunities for your business. By natively managing risk, ensuring economic predictability, and absorbing the friction of assembling tools, Nexcess delivers the simplicity to architect your vision and the performance to scale it. Cloud without compromise.