

# HIPAA

## Compliant Website Basics

What Healthcare Organizations Need To Know About HIPAA-Compliant Websites



by Erik Kangas, PhD



**LUXSCI**

[www.luxsci.com](http://www.luxsci.com)

# TABLE OF CONTENTS


---

|  |    |
|--|----|
| <b>INTRODUCTION</b> .....                                  | 3  |
| <b>CHAPTER 1</b>   |    |
| What Are HIPAA-compliant Websites? .....                   | 4  |
| HIPAA-compliance for Websites .....                        | 4  |
| HIPAA-compliance for Email .....                           | 5  |
| HIPAA-compliance for WordPress .....                       | 5  |
| <b>CHAPTER 2</b>   |    |
| What Is HIPAA-compliant Website Hosting? .....             | 7  |
| Components of a Solid Website Hosting Infrastructure ..... | 8  |
| Finding a HIPAA-compliant Hosting Provider .....           | 9  |
| <b>CHAPTER 3</b>   |    |
| What Are HIPAA - compliant Web Forms? .....                | 10 |
| <b>CONCLUSION</b> .....                                    | 12 |

# INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 laid out requirements for the healthcare industry to follow when working with protected health information (PHI) and, in this case, electronic-protected health information (ePHI). Any medically related data (including scheduling and billing) that is individually identifiable or traceable back to a patient falls into the ePHI category.

Before making any website-related decisions, your healthcare organization needs to understand the HIPAA rules and the best practices for implementing the necessary compliance measures.



Healthcare websites are a convenient way for patients to apply for health-enhancing programs, schedule appointments, contact medical practitioners, and more. However, considerable security is needed to protect this information.

# CHAPTER 1

## What Are HIPAA-compliant Websites?

Security for healthcare-related websites falls into two buckets: securing stored website data (e.g., on a server) and securing transferred data (e.g., website forms sending data through email). Users must take separate steps for each type of security.

### HIPAA-compliance for Websites

Websites can protect ePHI information by following the eight guidelines below:

- **Transport Encryption**  
Encrypt any data transported over the internet.
- **Backup**  
Back up all data to make it available for recovery.
- **Authorization**  
Issue unique access credentials so data can only be viewed by authorized personnel.
- **Audit**  
Log access to ePHI so that there's a record of who accessed it, when, and from where.
- **Integrity**  
Protect all data from unauthorized changes or tampering.
- **Storage Encryption**  
Encrypt data when it's stored or archived.
- **Disposal**  
Delete data in a way that makes it unrecoverable.
- **Business Associate Agreement (BAA)**  
Sign a BAA to serve as a record that both the organization and its third-party vendors (i.e., web hosting service providers) are aware of their responsibilities and obligations under HIPAA, especially in the event of a data breach.





## HIPAA-compliance for Email

While the above steps will help ensure your website is HIPAA-compliant, you still need to consider email. Having a HIPAA-compliant website doesn't automatically mean your email messages from that website are secure. If your website sends emails that contain ePHI, you need to take the following steps to ensure compliance:

### ■ Use a Third-Party Service for Web Forms

Many third-party companies can provide HIPAA-compliant data collection from your website's web forms, as well as compliant emailing and archiving of that data. Your developer can simply connect your web forms to such a service.

### ■ Use Secure Email Accounts

If your company has access to email accounts that can provide HIPAA-compliant outbound emailing, your web developer

can also connect your website to those accounts to ensure that emails are secure.

### ■ Direct Sending

If you need to send email directly from your web application, then your developers must themselves ensure they meet all the security requirements for HIPAA-compliant emailing, e.g., encryption, logging, authorized access, archival, etc. It's almost universally true that using the default email services available through web hosting providers will not ensure compliant email sending.

## HIPAA-compliance for WordPress

Many healthcare companies rely on popular third-party platforms such as WordPress to run their websites. However, these platforms are for general use and are not HIPAA-compliant. While



you can tailor WordPress for compliance, your organization should be very cautious. At the end of the day, you're responsible for any bugs or security mishaps on your WordPress site. Some additional steps you can take to safeguard your WordPress site include:

#### ■ **Ensuring Proper Access**

Ensure your HIPAA administrators properly vet users of your WordPress site. Nobody should ever be able to "sign up directly" on your site.

#### ■ **Performing Regular Upkeep**

Ensure that all WordPress and add-on (i.e., plugin) software is up-to-date. You should vet all plugins to ensure that they have been developed by respected, security-conscious organizations. The majority of WordPress security vulnerabilities involve defects in plugins.

#### ■ **Using Security Plugins**

Consider plugins like iThemes Security, Jituzu, or Duo Security that are either designed specifically for HIPAA-compliance or offer additional levels of security such as two-factor authentication.

#### ■ **Guarding Your Data**

WordPress will encrypt your data or provide much in the way of access auditing. If you plan to store ePHI in WordPress, you must take steps to encrypt your databases,

ensure proper backups and auditing are in place, and generally perform a detailed audit of the system to check that you meet all the HIPAA requirements.



# CHAPTER 2

## What Is HIPAA-compliant Website Hosting?

Whether you store your organization's healthcare information on in-house servers or with a third-party provider, you must comply with HIPAA's three fundamental requirements:

### ■ **Administrative Safeguards**

You and your hosting company must have procedures, policies, and processes in place to make sure all staff members working with PHI receive proper training and have oversight.

### ■ **Physical Safeguards**

Your website developers and your hosting company must have the proper system infrastructure in place, including audit controls, data storage, and encryption.

### ■ **Technical Safeguards**

Your website developers and hosting company must have procedures in place for

secure server management, including: server access controls, data redundancy, and business continuity options.

Note that the burden is on you and your website developers to make proper choices to ensure compliance. A hosting provider is not in control of your site, how it works, or what it does or does not do with PHI; they also don't control your particular business requirements with respect to disaster recovery, backups, etc. Your website developers must understand HIPAA and know how to architect the correct decisions.





## Components of a Solid Website Hosting Infrastructure

With these requirements in mind, let's consider what a hosting provider must have:

### ■ Access Controls

The provider must have proper procedures in place when it comes to controlling and validating which staff members have access to healthcare information that you may have stored in your account. This includes understanding which personnel (roles) have access to what data and in what capacity (e.g., server operations).

### ■ Accountability

The provider must keep accurate access and changes to the data and who has access to it. For instance, if the provider has to move your servers, who is moving them and why?

### ■ Firewalls

Hardware, software, and web application firewalls are crucial to ensuring that unwanted parties can't access your data. Implement firewalls system-wide.

### ■ Anti-Virus

Your servers should frequently and automatically scan for viruses and malware.

### ■ Off-Site Backup

Providers must have a backup of client data at a separate location in the event of a data breach, fire, or another event.

### ■ Private Hosted Environments

Choose your hosting infrastructure to be separate from all other clients (e.g., avoid shared servers). No other customers of your web host should have access to your servers.

### ■ SSL Certificates

Your provider must enable the use of secure sockets layer (SSL) certificates, which establish secure connections between a browser and a server. You should have SSL/TLS certificates installed so they cover all your website's pages.

### ■ VPN

Hosting providers should offer a virtual private network (VPN), which makes system



access more secure for end users since it doesn't require any software installation on the user's end.

## Finding a HIPAA-compliant Hosting Provider

Since no governing body certifies a hosting provider as HIPAA-compliant, it's up to you to find one that can fulfill your needs. When choosing the appropriate hosting provider for your organization, remember that the right one will:

### ■ Follow HIPAA's Four Rules

HIPAA has four rules that govern how to handle PHI: the Breach Notification Rule, the Enforcement Rule, the Privacy Rule, and the Security Rule. It's hard for providers to adjust their server infrastructure to accommodate all four rules, so it's best to go with a provider who has built theirs with these in mind.

### ■ Have SSAE 16 Certification

The American Institute of Certified Public Accountants created the Statement on Standards for Attestation Engagements (SSAE). Many consider the SSAE 16 certification stricter than HIPAA compliance, so providers with this certification are more likely to be in compliance with HIPAA standards.

### ■ Willingly Sign a BAA

HIPAA defines technology companies that agree to work with a healthcare provider as "business associates" of that provider.



## CHAPTER 3

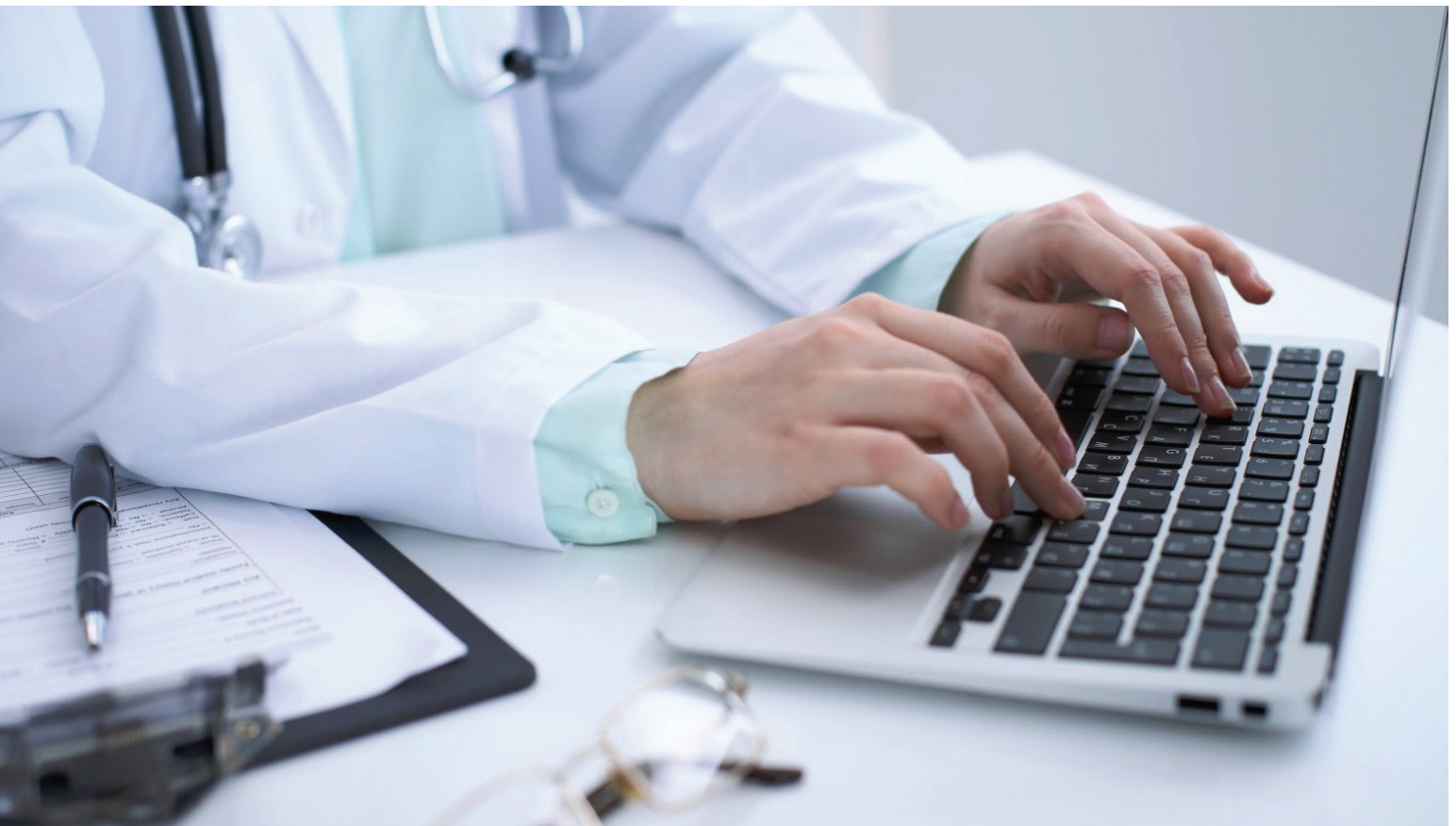
### What Are HIPAA - compliant Web Forms?

Whenever a website visitor is filling out information, such as scheduling an appointment or purchasing a prescription, they're using a web form. This causes security concerns because you have to consider how this information goes from the user's computer to your website. Can an unauthorized third party see and capture that data?

The foundation to securing a web form is an SSL certificate, which, as we already mentioned, your web hosting provider can install. However, having an SSL certificate on your website isn't enough. It's important to maintain two general rules:

Ensure that people can connect securely to your web form.

Ensure that people can't connect non-securely to your web form.





Ensuring that people can connect securely means using absolute links instead of relative links. If a user goes to your web form from a non-secure page, never direct them to a non-secure version of your web form (although we will say again that all pages on your site should have an SSL certificate).

Ensuring that people can't connect non-securely means blocking access to your web form through non-secure connections or redirecting non-secure connections to secure ones. This is called "locking down," or enforcing the use of SSL to access the web form, and you can do this in the following ways:

### ■ **Store SSL Pages in a Separate Location**

Some web hosting providers can configure your site so that secure and non-secure pages will store in separate directories. For any requests made for the non-secure version of your web form, a "Page Not Found" error will result.

### ■ **Use Scripted Pages**

For web forms that server-side scripts (e.g., Java, PHP, Perl, or Python) generate, the script can check to make sure the request is secure. If it's not, the script can send the user to the secure web form or return an error.

### ■ **Secure All Pages**

Taking the above to the next level, you can set up your site so that all requests for non-secure pages (including your web form) will redirect to the secure version.

- Ensuring secure submission of the web form data from the end user to your web serve
- Ensuring secure storage of all PHI that will reside on that server or other locations
- Ensuring secure transport of that data as email, FTP, SQL, or other protocols deliver it
- Ensuring that data posts are properly logged and audited
- Ensuring that you keep archived backups of all the posted data, etc.

Using web forms that collect ePHI is very useful but you must treat them very carefully. Unless your web developers are building a HIPAA-compliant framework that can handle all these points, we recommend using a third-party, HIPAA-compliant form processing system to handle your form data for you.

Securing access to your web forms is, unfortunately, only part of the battle, the "easy" part. When connecting PHI through a web form, you must consider all the following, as well:

# CONCLUSION

## Tips for a Compliant and Secure Website

Whether your organization has an existing website or is building a new one from scratch, ensuring HIPAA compliance requires high-level planning before diving into the security details. We've provided a few tips to help you to start planning or reviewing your website's compliance.

## Start with the Most Common Areas of Noncompliance

Start reviewing the most common vulnerabilities of basic websites.

The most common HIPAA issues include:

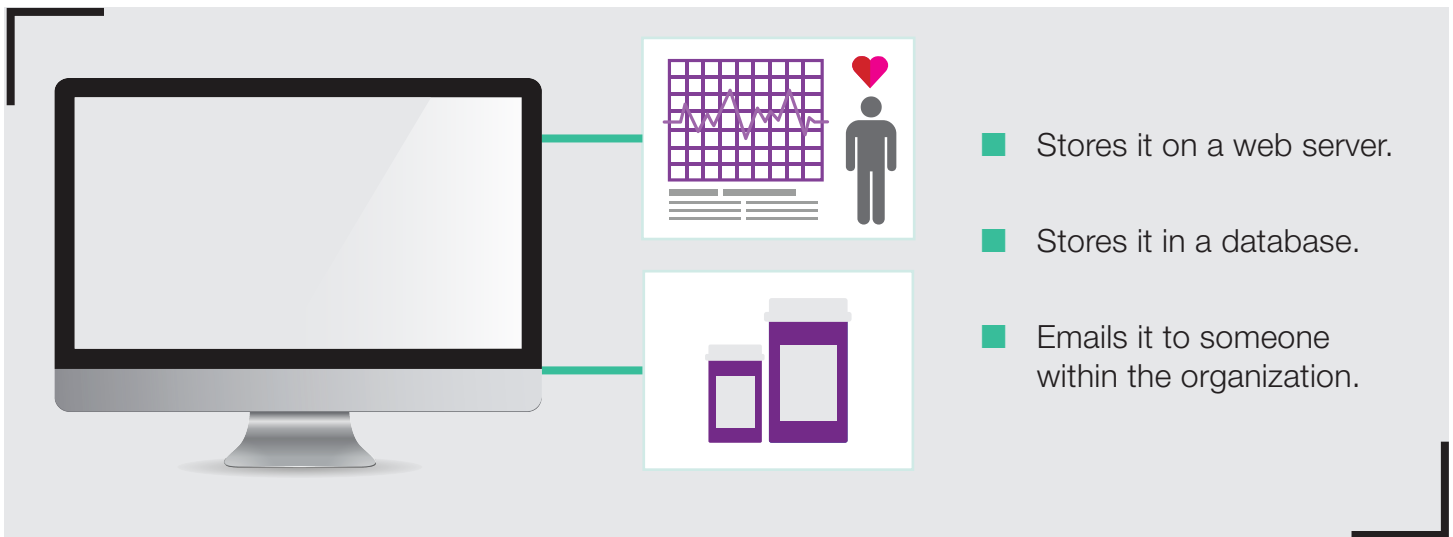
- Lack of Transport Encryption
- No Data Integrity Assurance
- No Storage Encryption
- Lack of Access Control and Auditing
- No Vendor BAA

It helps to have a place to start when talking with providers about HIPAA compliance and what types of services their companies offer.



## Understand How to Handle ePHI

Once you send a patient's information from a web form to your website, what does your organization do with that information? Most likely, your organization does one of the following:



Understanding how to handle this data will dictate what security measures you should take. Storing data on a web server, for example, means you may need to encrypt data, and downloading information from that server needs to be a secure process. Storing information in a database means you need to address database secure storage issues.

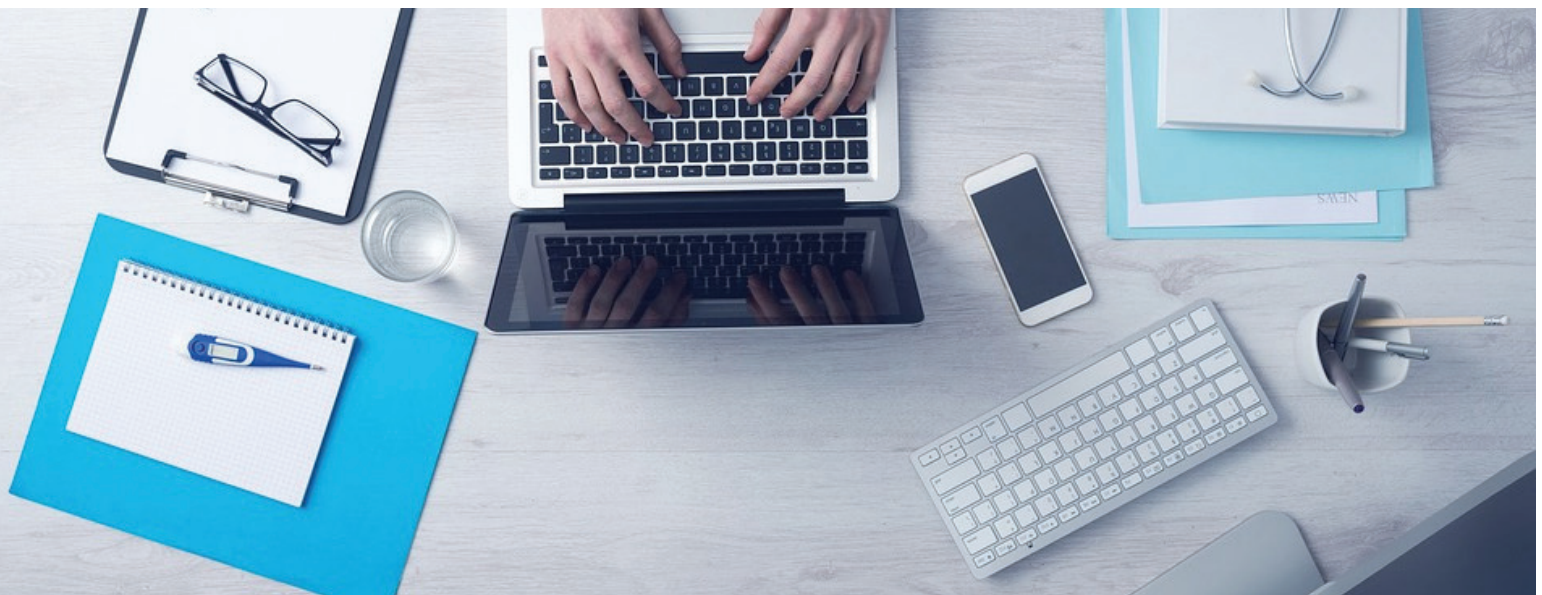


## Inform Developers of HIPAA Requirements

Developers who aren't familiar with HIPAA compliance may miss requirements that can leave your site vulnerable and leave you liable for any breaches. Common oversights include:

- Lack of audit trails for logins and PHI access. You need to archive for up to 10 years.
- Lack of emergency access to PHI.
- Lack of assurance that every person has a unique login to access your healthcare system.
- Lack of adequate protection for stored data.

Securing your healthcare organization's website requires a lot of technical know-how. Third-party providers, developers, HIPAA experts, and internet security professionals will all become involved in setting up your website. Understanding how HIPAA compliance affects the design of your website empowers you to coordinate everyone's efforts. After all, you understand the importance of securing your patient's data. Putting this into practice is what HIPAA compliance is all about.







## Have Additional Questions? We're Happy to Help!

Call: **+1 800-441-6612**

Email: **sales@luxsci.com**

Web: **luxsci.com**

## Solutions to Ensure Your Private Information Stays Private:

- Secure Email
- Secure Websites
- Secure Web & PDF Forms
- Secure Text
- Secure Chat
- Secure Email Marketing
- Secure Video

LuxSci is your trusted leader for secure email, data and communication solutions. LuxSci helps ensure that "what's private stays private." Find out why LuxSci is the go-to source by the nation's most influential institutions in healthcare, finance and government for comprehensive, flexible, and easy-to-use secure solutions.

MEDICAL

MEDICAL