LayerCompliance™

Top 4 Best Practices

FOR HEALTHCARE BUSINESS WEBSITES

CAEK™

INTRODUCTION

Marketing is an important part of your practice, and for most healthcare practices that means having a website. Unfortunately, internet-facing servers are usually first-in-line for a cyberattack. Internet-facing servers provide multiple doors into the network and the data transmitted, accessed, or stored in devices connected to that network. There are several practical steps that healthcare offices may take to protect their sensitive data and comply with HIPAA security regulations. As with all information systems, a healthcare organization's website must be included in their HIPAA risk analysis, and while this article does offer some suggestions that may help an organization in determining their level of risk, this article does not replace performing a risk analysis, identifying and implementing all appropriate safeguards, or ongoing risk management of your website.

#1. Separate Internet-Facing Servers from Your Practice Network

In companies with a large IT staff and budget, websites are on servers that are separate or segregated from the company's internal network(s). That way, if an attack is successful on one of the internet-facing servers, it can't access critical systems and sensitive data. For smaller healthcare organizations, maintaining separate or segregated networks can be expensive, that's why using a reputable website hosting service may be a cost-effective option.

Email can be, but does not have to be, hosted on the same server or with the same hosting company as your website. Most healthcare organizations' email systems are protected health information (PHI) systems, and therefore, may need multiple security controls, policies, and a business associate's agreement with the email hosting provider. Again, your email system should be part of your HIPAA Risk Analysis.

#2. Limit Web-forms and Online Payments

It seems like all websites have contact forms, and some healthcare providers also have appointment request, new patient, and payment web-forms on their websites. These forms can represent your biggest area of risk because the website is accepting data entered by unknown persons or systems. Attackers can use these forms to attempt to "inject" malicious code into the application or system.

Web-forms also allow your patients to enter protected health information, even if your contact form does not specifically request it. You may be required to protect any health information entered into a form on your website. That means that the data must be encrypted when transmitted. If the data is stored on the webserver, it must be protected, and the web hosting company may be considered a business associate. If the form data is emailed to your office, the email message may need to be encrypted.

Accepting payments by credit card and other payment methods may require compliance with another data security standard, Payment Card Industry (PCI). Failure to adhere to these standards, and protect credit card information, can have an impact on your practice's ability to accept credit cards online and in your office.

In reviewing all of the forms on your website, consider how necessary they are to your practice. How often are they used? Does the use justify the cost for implementing the appropriate safeguards and/or a potential data breach?

#3. Keep Your Webserver, Content Management, and Web Development Systems Up-to-Date

Your webserver needs to be patched with the latest security updates, just like all of your other systems. This includes the operating system and webserver, such as IIS or Apache. Most of today's websites are built using content management systems, such as WordPress and Joomla. These programs also have frequent security updates to the main application and third-party plug-ins that may be used on your website. Additionally, your website developer may use web content authoring tools that require security updates that may include updates to the website pages.

It is important that you determine who is responsible for ensuring all of these systems and applications are updated with the latest security patches. Review any contract or service level agreement (SLA) to verify that these updates are included and how often they will be performed. You may also request that the person responsible for installing these updates notify you whenever updates are scheduled and completed.

#4. Prepare an Incident Response Plan

Unfortunately, no matter what preventative measures you have in place, your website may be successfully attacked, hijacked (redirected to another site or content replaced), or taken offline. You need to have a response plan in place to handle these types of incidents, including but not limited to, contact information for the web hosting company, webmaster/web developer, and appropriate members of your staff. If you have a web monitoring service or process in place, you should keep the contact information for the appropriate member(s) of your incident response team up-to-date and identify the process for contacting the team during non-business hours.

Note on Patient Portals

This article does not address the requirements for patient portals and other PHI applications that may be connected to your electronic health record (EHR) system or practice management system. PHI systems should be included in your HIPAA risk analysis and risk management compliance program.

DO YOU HAVE SOMEONE TO CALL?

A marketing website is just one of hundreds of issues healthcare providers face in protecting their patients' data and complying with the HIPAA Security Rule. Do you have someone to call when you need help? Providing the tools and expert help your staff needs is critical to implementing a successful HIPAA security program in your practice. Let LayerCompliance™ help you get in and stay in compliance. Contact us today to get started (800) 334-6071

LAYERCOMPLIANCE™– A COMPREHENSIVE PROGRAM

CONSULT-LEVEL SERVICE. COST EFFECTIVE PRICE.

Risk Analysis
A full Risk Analysis that assesses systems and provides both HIPAA Security compliance and threat analysis.

Policies & Procedures
Custom HIPAA Security policies based on your individual organization—not generic templates.

Implementation
You can document HIPAA Security compliance activities, including the implementation of policies and security measures.

Risk Management
A once-a-year audit or assessment isn't enough. Breaches can happen every day and you need to stay in compliance all year round.

With LayerCompliance™, organizations can get the expert help and tools they need to get in and stay in compliance.

Live Support
Our team is ready to assist with HIPAA Security questions, incidents and potential breaches

HIPAA Security Training
We provide HIPAA Security awareness & security policy staff training

LAYERCOMPLIANCE™

800.334.6071