LayerCompliance™

Top 5 Best HIPAA Practices

FOR SOCIAL MEDIA

CAEK™

INTRODUCTION

Social media is an important part of any business today. Unlike other types of businesses, healthcare providers and covered entities must have a clear policy and procedure for using social media or face thousands of dollars in HIPAA penalties and other costs associated with a breach of protected health information.

This article reviews the top five best HIPAA practices for social media to consider when creating your HIPAA policy and procedure for your practice's social media.

#1. Policy should document type of information that is allowed for each social media platform

Sharing pictures of happy patients and their stories can promote good health as well as your business; however, anything shared on the internet is "forever," and social media platforms have various privacy and usage policies for images uploaded into their systems. Images you post on Facebook, Twitter, or your own website can be downloaded and used by anyone on the internet. Additionally, using full names can put your patients at risk to identity theft. For instance, if you quote one of your patients and provide her full name, you may be creating an opportunity for an identity thief to use your name to steal her information.

"Hello Ms. Donovan, this is Julie from Dr. Thompson's office. I need to verify your social security number and insurance information."

#2. Review form(s) authorizing use of images and information for marketing purposes with legal counsel

Because anything shared on the internet is "forever," and once it is shared you have limited control over the use of the image or information, make sure the forms your patients sign to authorize use of their information for marketing purposes are reviewed by an attorney who is well versed in both privacy and social media. Remember, it's not just your patients that may need to authorize the use of images and information, you may need authorization from your employees as well. Make sure you have a clear policy and procedure for verifying that the use of the information complies with the signed authorization. Your policy and procedure should include retention of the authorization; your legal counsel may advise you to keep the signed forms longer than what is required for medical records.

#3. Protect social media account and access

The person(s) authorized to access and manage your social media accounts should be trained on your policy. If you've hired a third party to manage your social media, verify that they understand your policy and procedure. You may want to have your attorney review the third party contract to verify that it includes following your policy. Anyone accessing your social media accounts should also follow best practices for login credentials and passwords to protect against unauthorized access. Hacked social media accounts can damage your business and reputation.

#4. Monitor your social media accounts frequently and have an incident response plan

Frequent monitoring of your social media accounts can help limit the impact of unauthorized content that does not comply with your social media policy. Mistakes can happen, such as a social media manager posting a personal message on your business account instead of his or her personal account, a social media account hacked by malicious person(s), or the wrong image uploaded to a webpage. For each social media platform used by your practice, be sure that your incident response plan includes the information and process to verify ownership of the account, process to remove content or disable account, and up-to-date contact information for management and social media manager(s).

#5. Review and update policy before using new social media platforms and features on current social media accounts

New social media platforms and features are available almost every day. Before starting something new, review the planned use and your existing social media policy. You may need to update your policy or reconsider the use of that new feature or social media platform.

DO YOU USE TEMPLATE POLICIES AND PROCEDURES?

The Office for Civil Rights (OCR) has fined providers for using sample policies and procedures that are not followed. We provide custom policies and procedures and the ability to document that your staff is complying with your policies. 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