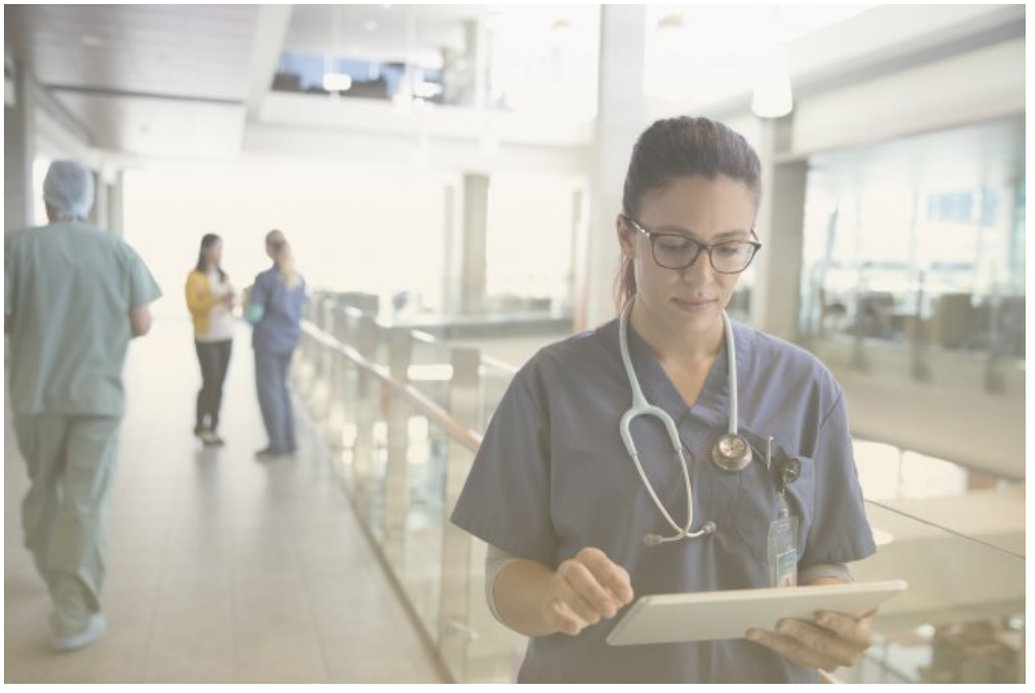
4 Common HIPAA Compliance Violations and How to Avoid Them

By BECKY LAWLOR - Contributor

Healthcare organizations that regularly handle sensitive patient data are faced with the difficult task of aligning with HIPAA regulations. No healthcare organization, no matter how small or large, is immune from the costly penalties for non-compliance. The Department of Health and Human Services (HHS) recently reported that Anthem paid a $16 million settlement to the Office for Civil Rights (OCR) for non-compliance. And this steep fee wasn't all: The combination of litigation fees, high costs of resources and labor, as well as a loss of trust cost Anthem significantly more than just their settlement payment, ultimately serving as a reminder of the significant HIPAA violation consequences healthcare providers may incur if they don't meet established requirements.



With a UCaaS platform in place, healthcare organizations can avoid common HIPAA compliance violations.

Here's a look at some of the most common HIPAA compliance violations, along with advice on how to remedy non-compliance or better prepare for HIPAA compliance risks.

A New Era of Communications

Adopting a UCaaS system is just the first step. Learn how a full digital transformation can benefit your organization.

1. Lack of Planning

When it comes to security risk management, the adage that "failure to plan is planning to fail" may unfortunately apply to many healthcare organizations. In a 2017 OCR audit, the HHS reported that not a single organization it audited received a full compliance rating for performing an information risk analysis. An even greater number of audited groups had made limited or no attempts at complying with HIPAA by establishing or maintaining an information risk management plan.

Given the inherent risks of hacking and other types of data breaches for electronic patient health information (ePHI), organizations must spend the resources and time to consider what security risks they face and how they can best manage or avoid them. Conducting a risk analysis and implementing a management plan is a key part of HIPAA compliance regulations. It can also help identify and address other common areas of concern for HIPAA compliance.

Having multiple channels for internal and external communication like SMS, email, voice, or chat, for instance, can leave an organization at risk. Instead of managing the data flow for each of these channels individually, healthcare groups can unify front-desk and patient-care operations through a cloud-based unified communications-as-a-service (UCaaS) platform. Using a UCaaS platform means that the organization only has to manage one centralized communications system, making it easier to maintain compliant practices. Performing a risk analysis and modernizing legacy systems allow organizations to identify ahead of time how their communications and data management might be better served with a UCaaS system in place.

2. Poor Mobile Protection

Today's medical professionals are increasingly using mobile devices like smartphones and laptops to collaborate with patients and colleagues and manage day-to-day workflows. While mobility can certainly help improve remote patient care by allowing doctors and

nurses to work with patients who are otherwise unable to reach an office, it's also another factor that healthcare organizations need to manage when it comes to HIPAA compliance.

To reduce mobile risks, organizations can:

- Conduct a risk analysis and implement a risk management plan.
- Develop device controls such as encryption, multi-factor authentication and remote wipe capabilities.
- Ensure any business associate has the proper security measures in place.
- Train employees to use only pre-approved HIPAA-secure applications to exchange ePHI.

One way to take these steps is by adopting a UCaaS system with integrated call metrics so that an organization can sync all mobile devices with its current application. By funneling all call data through one native reporting dashboard, the organization not only receives useful information on incoming and outgoing calls, but also can require multi-factor authentication on all connected devices, reducing the risk of HIPAA non-compliance.

> *With its ability to centralize internal and external communications and improve risk management and day-to-day operations simultaneously, UCaaS can be the key to healthcare HIPAA compliance.*

3. Improper BAA Vetting

Using business associates like cloud service providers is a common and necessary practice among health organizations. Cloud-based technology can make healthcare workers more productive, save the organization money, and improve patient communications through technologies such as SMS alerts. Because the HIPAA security rules mandate business associate agreements (BAAs) with all third-party vendors, however, it's important to ensure that BAAs also meet HIPAA security rules.

A good BAA should protect both parties in the event of a breach. It's important to make sure the agreement covers key points of liability. For starters, the BAA should include an acknowledgment that both the covered entity (the healthcare organization) and the business associate (the third-party provider) must comply with HIPAA regulations. Second, the agreement should include explicit language around who is responsible for a breach of protected health information so the right entities are held liable for any loss or poor management of data. Finally, the BAA should outline how the business associate's solutions abide by HIPAA standards or provide verification of HIPAA compliance through a certifying third party like the Health Information Trust Alliance (HITRUST). Establishing a solid BAA agreement can go a long way toward managing compliance risks.

4. Inadequate Employee Training

According to Health IT Security, 58 percent of threats to sensitive data come from insiders, making employee negligence one of the main causes of non-compliance risk in healthcare. Most of these incidents are accidental, such as losing a device, misinterpreting access privileges, or mishandling data.

Better employee training is the best defense against these types of accidental non-compliance. Make sure employees understand the importance of HIPAA compliance and the significant penalties for non-compliance of HIPAA. Train them on how to best protect mobile devices with multi-factor authentication, how to use secure applications to exchange ePHI, and how to avoid other risks like phishing that can lead to data breaches. With the right employee training programs in place, the organization will be better equipped to manage compliance.

The OCR shows no signs of abating its enforcement of HIPAA compliance. The best defense against an audit is to meet HIPAA compliance requirements — and having a UCaaS system in place can be the best first step. With its ability to centralize internal and external communications and improve risk management and day-to-day operations simultaneously, UCaaS can be the key to healthcare HIPAA compliance.