8 Things Your Practice Should Do to Stay HIPAA Compliant

By Angela Watkins

PHYSICIANS PRACTICE

Hire Professionals

"For technical issues involving data security, don't go it alone. The money you spend on hiring a HIPAA consultant or managed service provider to implement necessary protections, can save you money down the road, including the expense of litigation and fines."
-Barbie Hays, coding and compliance strategist, AAFP

"In my experience, most practices make it a priority to identify and consult with experts who are vital in the maintenance of the business, such as an accountant, attorney, etc. The critical role of maintaining and safeguarding patients' records should require an equal investment and appreciation of the expertise of professionals who can help you protect your most important assets."
-David Holtzman, vice president of compliance strategies, CynergisTek

Monitor Employees

Hacking of patient records doesn't always come from the outside. Potential problems might also arise from within, such as employee snooping.

"By conducting regular audits of who has access to systems and databases can provide a practice with information of inappropriately accessed medical records."
-Ericka L. Adler, partner, Roetzel & Andress, Chicago

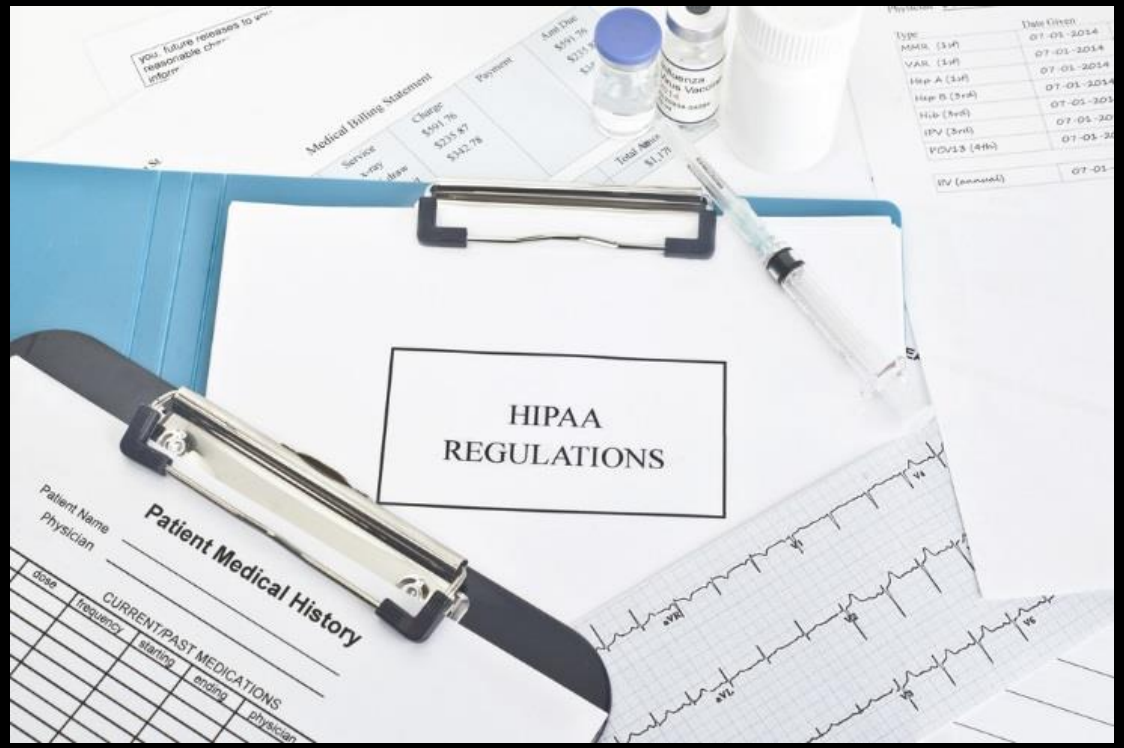
"Practices should have policies and procedures in place for modifying and/or terminating users' rights of access. Compliance requires ongoing reviews of changes and updates to a practice's handbook as well as training."
-Hays

Encrypt and Back Up Data

"Although practices understand the importance of encryption for in-office computers regarding electronic Protected Health Information (ePHI), sometimes mobile devices, such as cell phones (including personal cell phones) and tablets are overlooked. All devices used in the communication of ePHI should be encrypted, even if someone from the practice is using their own personal device."

Adler

Compliance Basics



"Compliance requires ongoing reviews of changes and updates to a practice's handbook as well as training."
-Hays

"There are sophisticated training and information programs [on compliance] available through the American Medical Associations, the American Association of Family Physicians, and other specialty associations."
-Holtzman

Know Your Business Associates

"It is critical for practices to know who is handling PHI and obtain assurances that the information is protected. Practices should have business associate agreements in place. HHS offers model business associate agreement language."
-Adler

"Just as you update your policies, procedures and training, you should also update your list of business associates and make sure an agreement has been signed."
-Hays

The Value of Ongoing Security Risk Assessments

"Your practice can't protect ePHI if you don't know where your data is. Regular security risk assessments help identify exactly where ePHI data is located."
-Hays

"A security risk assessment not only helps identify vulnerabilities that might pose a risk to the information system, but it helps identify the current protections in place to protect data."
-Holtzman

Sharing Information

"Be proactive by creating a 'culture of compliance' in your practice that continually raises employee awareness of privacy and security. There are many resources available to you, including online resources from the Office of Civil Rights, that can help build that culture. Some online resources also provide CME credits to professional employees."

-Holtzman

Prevent Ransomware Attacks

"Practices and their business associates should install anti-malware software as well as educate staff on data security practices, such as avoiding suspicious websites. In addition, practices should make regular backups of all systems and critical data."
-Adler

"Provide the least access possible for employees to do their jobs. Limiting access means that if those users become infected, there's less data that the malware can infect."
-Hays.