ACUPUNCTURE Today

RULES & REGULATIONS

Here's How to Avoid the Three Most Common (and Expensive) HIPAA Failures

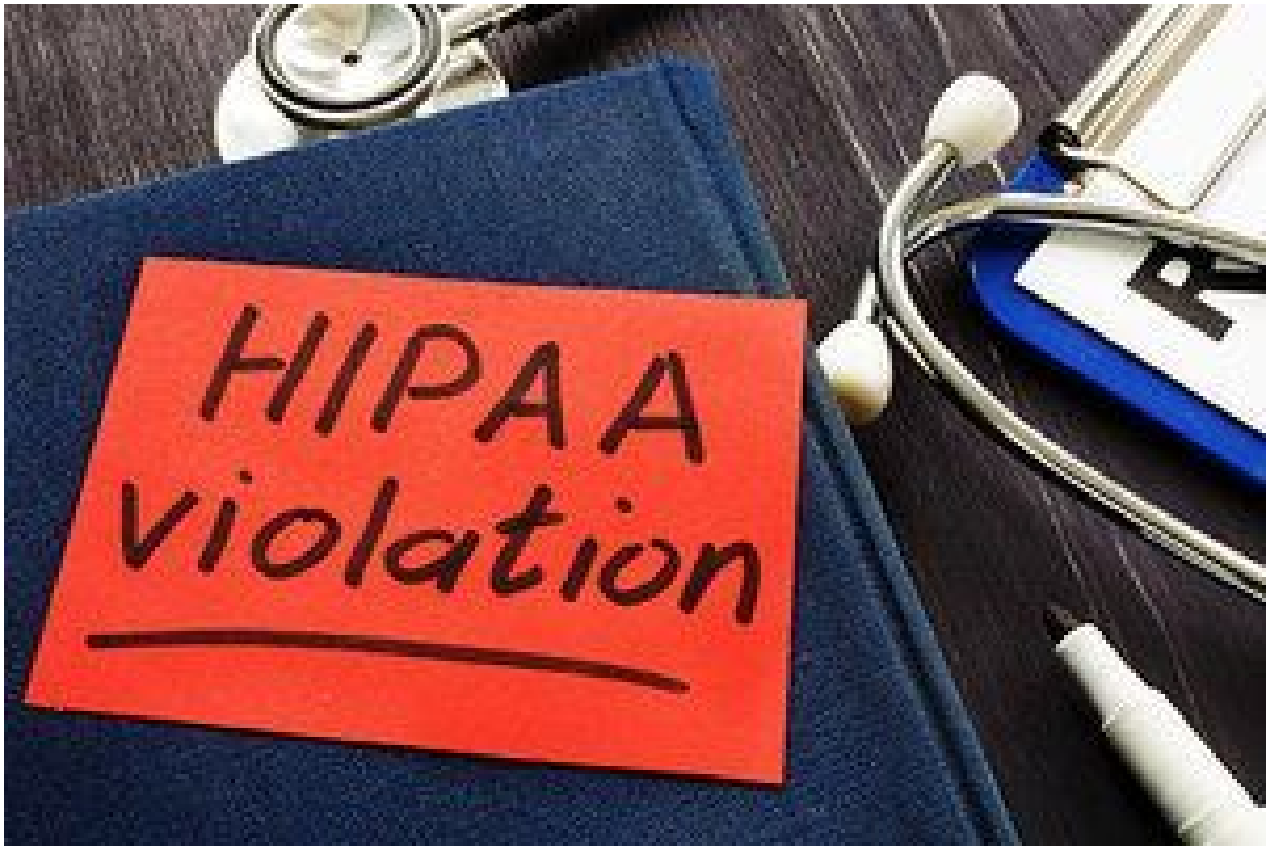
David Bibbey, Dipl. Ac., LAc

Editor's Note: This is the sixth article in David's 2022 series devoted to assisting acupuncture practitioners in understanding and complying with different aspects of the Health Insurance Portability and Accountability Act (HIPAA). The first article appeared in the February 2022 issue.

The most common and expensive HIPAA violations involve three critical areas: failure to perform a data security risk analysis; failure to sign a HIPAA-compliant business associate agreement (BAA); and improper disclosures of protected health information (PHI). Acupuncturists can easily avoid making these mistakes by understanding what is required and following a few simple steps.

#1: Failure to Perform a Data Security Risk Analysis

Failing to document a risk analysis is one of the most common HIPAA violations that results in a financial penalty. Completing a security risk analysis is not difficult or expensive, but it does require some expert help. Small and solo practices can visit www.hhs.gov or contact a HIPAA compliance consultant to determine the best option based on how their individual practice creates, shares, stores and destroys patient data. (Facilities and larger practices usually have in-house security and audit officers who complete this task.)



Health care practices are required to keep records of their risk analysis documentation from the previous six years. If a risk analysis is not being completed routinely (annually), then the provider is unable to identify, document and fix technical or personnel issues that threaten the confidentiality, integrity and availability of PHI.

HHS and the Office of Civil Rights (OCR) levy the highest fines and penalties in these instances of "willful neglect" to highlight common HIPAA violations and raise awareness of the need to comply with specific aspects of HIPAA rules.

How to Minimize Your Risk

Completing and documenting a security risk analysis (SRA) is a simple pass / fail element for HIPAA compliance. Either providers complete and document the SRA or they don't. Proof that the SRA has been completed must be documented and the records / reports need to be retained for six years. The actual analysis is performed by completing a web or app-based survey-style questionnaire that assesses and analyzes seven critical areas related to your practice's privacy and security procedures.

A report will be generated for the provider that highlights areas of successful HIPAA compliance and areas that need more work. HHS provides a sample of this questionnaire, but states on the government website that the sample language is not intended to replace an actual SRA.

Small and solo health care providers should consult with a HIPAA compliance expert who can provide them with an analysis model suitable for their practice size and budget. The annual cost can range from $200 for a small / solo office to $2,500 for a medium-sized practice with multiple types of providers and staff. Completing the analysis questionnaire usually takes 60-90 minutes.

#2: Failure to Enter Into a HIPAA-Compliant Business Associate Agreement

The failure to enter into a HIPAA-compliant business associate agreement (BAA) with all vendors given access to PHI is another common HIPAA violation. Even when business associate agreements for all vendors are on file, these may not be HIPAA compliant, especially if the agreement has not been revised after the Omnibus Final Rule.

This rule expanded the definition of "business associate" to mean a person or business that creates, receives, maintains, or transmits protected health information to perform business functions on behalf of a health care practice, like billing, accounting or legal work. A trusted consultant or attorney can be helpful when reviewing a BAA for accuracy and completeness.

Health care providers need to be certain that all of their vendors with access to PHI or ePHI are properly protecting patients' health and personal data. This also means questioning vendors about their staff training, use of encryption, systems' login access, and any data security audit outcomes.

How to Minimize Your Risk

Failure to enter into a BAA with vendors is a common HIPAA violation that results in fines. For example, say your practice uses XYZ Billing Company to process insurance claims for patient care. This business relationship requires your office to disclose and share PHI with XYZ Billing Company.

Prior to sending and sharing any PHI, you are compelled under HIPAA to have the owner/director of XYZ Billing sign a BAA, which requires the company to use safeguards that protect and limit the use of your patients' health and private information. You are also required to conduct "due diligence" to assure that XYZ Billing is handling your patients' info securely; and that it has processes in place to respond to data vulnerabilities, threats, and breaches. A signed and updated copy of the BAA must be on file in your office.

#3: Failure to Prevent Disclosures of Protected Health Information

Any unapproved disclosure of protected health information that is not permitted under the HIPAA privacy rule can attract a financial penalty. This typically includes improperly disclosing patients' PHI, illegal disclosures following the theft or loss of unencrypted computer devices, careless handling of PHI, disclosing PHI unnecessarily, not adhering to the "minimum necessary" standard, and disclosures of PHI after patient authorizations have expired.

HIPAA requires health care providers and their staff to follow a written policies and procedures manual that defines how, when and by whom PHI and ePHI may be disclosed. Standard language is often used in these clinic manuals, but the clinic director should routinely review the manual for accuracy, to update changes, to educate staff, and to document office training.

How to Minimize Your Risk

Improper disclosures of PHI happen when patient information physically leaves your office, or is otherwise communicated or shared in a manner not authorized by the patient nor exempted under state or federal law.

As an example, texting patient information may seem fast and effective, but it also gives others the ability to access patients' PHI. You can't put a patient's name or information in a text. If you do and you're caught, it can be a $5,000 fine per violation per text. And legally, you're required to report those violations.

There are programs that encrypt the information and allow it to be texted without concern. But the problem here is that it needs to be installed on the wireless device of *both* parties, and it rarely is.

Texting PHI is just not HIPAA friendly. See the HIPAA breach notification rule, *45 CFR §§ 164.400-414*.

Author's Note: For more information related to this article, please visit www.patientdataprotection.com or call Matthew Fiorenza, compliance and security specialist, at 352-268-5088, ext. 4.

OCTOBER 2022