ACUPUNCTURE today

HIPAA 101

State Patient Health Information Privacy Laws: Know What's Required

David Bibbey, Dipl. Ac., LAc

Editor's Note: This is the third in an important monthly series of articles 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.

HIPAA is a federal statute that applies to health care providers who collect, manage and share patients' protected health information (PHI) and their business associates, but it is not the only legislation covering the privacy and security of health care data. HIPAA sets minimum federal standards for health information privacy and security, but individual states have implemented more stringent requirements.

Therefore, acupuncturists must provide and document that they and any staff have completed an annual review or training to comply with their individual state laws. For instance, health care practices in Texas are required to complete and document training on *Texas HB 300* and the requirements of the *Texas Medical Records Privacy Act*, which provides more strict minimum standards than HIPAA.

The Confidentiality of Medical Information Act (CMIA) in California protects the privacy of medical information (in electronic or paper format) from unauthorized access and disclosures. The California state law mirrors HIPAA's privacy and security rules and includes its own Physical Safeguards – Health and Safety Code § 1280.18, which requires health providers to establish and implement administrative, technical and physical safeguards to protect the privacy of patients' medical information.

The Stop Hacks and Improve Electronic Data Security (SHIELD) Act in New York improves privacy protections for state residents and strengthens the state's data breach notification laws to ensure they maintain pace with current technology. The SHIELD Act expanded the definition of covered entities to include any person or entity that holds the private information of a New York State resident, and requires all businesses to "develop, document, implement and maintain reasonable safeguards" to ensure the confidentiality, integrity and availability of personal information.

A written data security program must be developed which incorporates all SHIELD Act requirements. The responsibility for implementing and administrating the program must be assigned to an individual, who oversees employee training on SHIELD Act requirements. The act also expanded the definition of personal information to include email addresses and usernames, along with the associated password or security questions' answers that would allow the account to be accessed.

Most states have or soon will pass legislation designed to enhance consumers' and patients' data privacy. Any business that collects and maintains personal identifiable information (PII) or

protected health information (PHI) needs to have written data privacy and data security policies and procedures on-hand and available for reference and staff training to meet federal and state law requirements.

To maintain HIPAA compliance in your office, in addition to reviewing any annual HIPAA changes that affect your patients and practice, you should review your state's personal data and medical privacy laws to determine if your policies and procedures meet the current requirements. Be sure to share any policy updates and changes with your staff and document that HIPAA refresher training has been completed.

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

APRIL 2022