ACUPUNCTURE Today

COMPLIANCE 101

Have You Documented Your HIPAA Security Risk Assessment (SRA)?

David Bibbey, Dipl. Ac., LAc

Editor's Note: This is the fourth in an ongoing 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.

All health care practices, including acupuncturists, who collect, receive, store, transmit or destroy ("de-identify") patients' protected health information in electronic form (ePHI) for insurance referral, authorization or claims purposes, are required to complete a HIPAA Security Risk Assessment (SRA).[1]

So, what does this involve? The key thing to remember is that this assessment generates a report, which a) confirms that your clinic complies with the HIPAA security rule; and (b) documents how you achieve and maintain that compliance.

What an SRA Should Include

Data Collection: Identify where the e-PHI is stored, received, maintained or transmitted. The data on e-PHI gathered using these methods must be documented.

It is important for all acupuncturists to remember that no matter the size of your office or staff, privacy and security rules under state and federal law must be observed and followed, whether you are a solo practitioner or work in a large group with staff. The HIPAA privacy and security rules are intentionally flexible and scalable to cover every type and size of health care practice.

Identify and Document Potential Threats and Vulnerabilities: Identify and document reasonably anticipated threats to e-PHI.

Assess Current Security Measures: Assess and document the security measures used to safeguard ePHI, and if current security measures are configured and used properly.

Determine the Likelihood of Threat Occurrence: Assess the probability of potential risks to e-PHI. How likely can your data be breached?

Determine the Potential Impact of Threat Occurrence: Assess the potential impact resulting from a threat triggering or exploiting a specific vulnerability.

Determine the Level of Risk: Assign risk levels for all threat and vulnerability combinations identified during the risk analysis. Document corrective actions.

Periodic Review and Updates to the Risk Assessment: Update / document security measures "as needed."

Common Security Risks and Next Steps

The most common security risks identified include lack of adequate written policies and procedures, missing encryption, lack of emergency preparedness, and lack of mobile device management.

The Office of the National Coordinator (ONC) for Health Information Technology developed an online SRA training tool in 2002 to help providers understand the SRA criteria. Unfortunately, this tool is missing critical elements: no sample policies and procedures, no action plan with tips to address risks identified in your report, and no tech support.

For these and other reasons, it's best to do your own research into how to complete a HIPAA Security Risk Assessment. You may want to reach out to an expert in the industry who can provide the tools you need to complete your SRA easily and efficiently.

Finally, your SRA findings may require you to update your HIPAA training and awareness program. Having solid policies in place is not effective if you are not documenting and communicating them. And from a compliance standpoint, if not documented and implemented, those policies don't really exist.

Reference

1. Guidance on Risk Analysis. U.S. Department of Health and Human Services (HHS): www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

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.

JUNE 2022