Codify
BY AAPC

Health Information Compliance Alert

Business Associates: Evaluate Your BAs' HIPAA IQ Before a Breach Happens

Hint: Understand what OCR means by 'satisfactory assurances.'

For covered entities (CEs), one of the most critical aspects of the job is protecting confidential patient information. And that's why it's essential that you know whether your business associates (BAs) and vendors really understand the importance of HIPAA compliance before you share protected health information (PHI) with them.

Reminder: A BA "is any person or entity that performs a function or activity on behalf of the practice involving the use and/or disclosure of PHI that is not a part of the practice's staff," reminds **Kent Moore,** senior strategist for physician payment at the American Academy of Family Physicians.

Additionally, because these BAs have access to your patients' medical records, they are subject to HIPAA.

Know These Facts on BAs

"HIPAA requires covered entities and business associates to obtain 'satisfactory assurances' that their vendors that need access to protected health information will safeguard that information appropriately," says attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida.

In the past, the HHS Office for Civil Rights (OCR) "has indicated that companies don't necessarily need to do much more than obtain a written business associate agreement from the vendor that complies with HIPAA and conduct a risk analysis," Hartsfield adds.

For example, consider the OCR guidance on cloud services providers (CSPs), Hartsfield suggests. "The HIPAA Rules do not expressly require that a CSP provide documentation of its security practices or otherwise allow a customer to audit its security practices," according to OCR.

However: As part of the HIPAA Security Rule, CEs and BAs are required to "conduct an 'accurate and thorough' analysis of the risks and vulnerabilities to electronic protected health information (ePHI)," Hartsfield reminds. "OCR has indicated that customers may ask vendors for 'additional assurances of protections for the PHI, such as documentation of safeguards or audits, based on their own risk analysis and risk management or other compliance activities,'" she says.

Remember: Not too long ago, OCR updated its guidance on the direct liability of BAs, clarifying which "party is ultimately responsible for satisfaction of various responsibilities and patient rights," explains HIPAA expert **Jim Sheldon-Dean,** founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont. "Where the BA is not responsible, the hiring entity is."

Consider asking your BAs these questions to test their understanding of HIPAA compliance before you add them to the payroll:

- What HIPAA Rules' safeguards do you employ to protect PHI/ePHI?
- Is it possible to review your HIPAA-compliance record?
- Are you willing to enter into a business associate agreement (BAA)?

- What tools and services do you offer?
- Do you perform an annual audit and analyze your risks?
- What kind of vetting do your employees undergo?
- Do you train staff on HIPAA compliance - and update when regulations change?
- Do you implement mobile device management?
- Are you aware of the spike in cybersecurity risks to the healthcare industry?
- What are your policies, procedures, and protocols for a data breach?
- Do you have an incident response plan, including a chain of command, in place?

Resource: Review OCR guidance on BAs at www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.