Codify
BY AAPC

Health Information Compliance Alert

HIPAA Quiz: Test Your HIPAA Security Rule Smarts

Tip: A business associate agreement means HIPAA applies to you.

Though HIPAA privacy violations are on the decline, data breaches are on the rise in healthcare. It's vitally important that your policies and procedures are up-to-date and meet the latest security requirements.

Check yourself on these HIPAA Security rule facts before you outline your 2018 protocols.

Question 1: The coding team, 123 Coders, process a lot of claims for our pediatric practice. They don't come into contact with any patients, but we do send them a lot of patient information electronically. Would they be considered a covered entity (CE)? Does HIPAA even apply to them since they don't seepatients?

Answer: No, their coders are not CEs, but they do handle electronic protected health information (ePHI), which makes them business associates (BAs). However, because they do carry out healthcare activities and see a myriad of personal data come across their screens, they are privy to HIPAA and must follow the Security rule requirements. You will need to institute a business associate agreement (BAA) with the company, ensuring they understand the importance of "potential risks and vulnerabilities to the confidentiality, integrity, and availability" of ePHI, according to the HIPAA Security rule.

See HHS guidance on BAAs and find a sample contract at: www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

Tip: Not everyone who interacts with your practice needs a BAA. Take the cleaning staff for example. "Business associate agreements include organizations that may create, receive, maintain or transmit health information," notes HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont. "The cleaning staff should be under a confidentiality agreement but not necessarily a business associate agreement."

Question 2: In our small practice, we all take turns being in charge of the data security. Do we really need to incur the expense of a "security officer?"

Answer: Yes, you absolutely need a dedicated HIPAA security officer. No matter the size or scope of your practice, if patients' ePHI is being held or transferred at your healthcare office, the HIPAA Security rule mandates the assignment. "A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures," notes the "Administrative Safeguards," section § 164.308(a)(2), of the HIPAA Security rule.

Tip: Remember, it will be your HIPAA security officer who acts as the liaison between the HHS Office for Civil Rights (OCR) and your legal team should a data breach occur. He or she must know your HIPAA compliance plan and speak to any issues that arise.

Question 3: We decided to just use the same password for all of our practice mobile devices to make access easier. Are we HIPAA compliant?

Answer: Yes and no. It is smart that you have instituted password protection on your mobile units, but sharing the same password is not a good idea. The fact that everyone in the office knows the password could hurt you down the pike. According to the HIPAA Security rule "Physical Safeguards," section § 164.310(d)(1), "a covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media."

Tip: Since more and more breach cases highlight the importance of multi-factor authentication, implementing strong

encryption and at-rest rules on your devices is critical. It is also optimal that you change the passwords monthly and limit mobile device and password access as well. These actions fall under mobile device management and your HIPAA security officer will be the go-to person.

Question 4: HIPAA security is really important to our flu clinic. Our new security official said we need to do a risk analysis more than once a year. Is that really necessary?

Answer: Yes, and the HIPAA Security rule suggests that covered entities and their respective staffs assess and analyze risk often. "Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to ePHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to ePHI," the "Administrative Safeguards," section § 164.308(a)(1), of the HIPAA Security rule indicates.

Tip: "Hackers are a step ahead of private practices, and they [physicians] easily fall victim to them," says attorney **Clinton Mikel** of The Health Law Partners, P.C., in the Southfield, Michigan office. "If the OCR investigates and finds over 500 individuals were affected, the first thing they will look for is the security risk analysis." Some items that might be on your risk checklist include:

- Identify any risks and how they would impact ePHI and your practice.
- Put a plan into action to combat the risks and enforce it.
- Document and list your risks and how your plan addresses them in writing. This is particularly important because the OCR will ask for this if there's a breach.
- Educate your staff, both clinical and administrative, on the ePHI risk issues and HIPAA.
- Make HIPAA security a priority in your office with measures that work.

Question 5: Our HIT security vendor insists we log unusual activity in our network, but it's so time consuming, and we've never had a breach. Would it really hurt if we just turned off the system on busy days and skipped the monitoring?

Answer: Actually, yes, it would greatly impact both your health IT security company and your practice IT and security officials from properly monitoring threats and inconsistencies within your network and systems. The HIPAA Security rule's "Technical Safeguards" section directs CEs on exactly what must be covered. The list includes these four essentials:

- Outline who has access to ePHI and devices.
- Utilize hardware, software, and protocols that log and monitor your system.
- Detail policies that instruct others on how ePHI is managed and disposed of properly.
- Ensure the protection of ePHI with technical measures against impermissible access and disclosure.

Tip: "Practices should be looking at the integrity of the systems, oftentimes they don't," warns compliance expert **Brand Barney, CISSP, HCISPP, QSA,** a security analyst with Security Metrics in Orem, Utah. And if you don't, Barney asks, "How do you know when there's a problem?"

For example: "They [systems] continue to blast with alerts but the staff has no training. They find it too noisyand turn it off. So when there's a real breach they have no idea," Barney cautions. "If you have no loggingand monitoring mechanisms, you are in deeper than you want to be." He adds, "I can't stress this piece enough. Properly log and monitor your networks and systems. Attackers are banking on you having no insight, then they walk away with your data, and you are none the wiser."

Resource: To find the complete summary of the HIPAA Security rule, visit www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.