Health Information Compliance Alert

HIPAA Quiz: Test Your Knowledge of HIPAA

Make sure your staff know the essentials to avoid a violation.

Even though you may think that you've got HIPAA wrapped up, compliance is something that should be part of your daily operations; moreover, your should revisit protocols frequently to ensure the entire staff is up-to-date and onboard.>

Here's why: A significant HIPAA slip-up can open your practice up to dozens of violations, wreaking both fiscal and personal havoc on your business. And beyond the damage to your finances and reputation, a breach can also put your patients in harm's way, exposing their protected health information (PHI).>

Front-desk staffers and seasoned clinicians alike need comprehensive HIPAA training. Consider adding these 10 questions to your next compliance training sessions:>

1. When do the HIPAA Privacy and Security Rules apply to PHI?>

a. Only at work or in the office
b. Sometimes during discussions of patients with my co-workers or other clinicians
c. When I transfer data electronically via text
d. Every time it is used, accessed, disclosed, transmitted, stored, or filed, both in person and electronically>

2. What constitutes PHI or ePHI?>

a. A patient's name on a prescription label
b. A patient's email address
c. A Social Security number
d. All of the above>

3. What is a way that you can legally dispose of ePHI under HIPAA?>

a. Delete a file from the computer
b. Physically destroy the storage device
c. Sell the hardware to another IT firm
d. None of the above>

4. What is not an example of a technical safeguard under the HIPAA Security Rule?

a. Log and monitor network activity
b. Use mobile devices to assist patients
c. Utilize multi-factor authentication for passwords
d. Back up and secure data at a remote location>

5. How many years does the HIPAA Privacy Rule protect a patient's PHI after he passes away?>

a. 10 years
b. 25 years
c. 50 years
d. 100 years>

6. A nurse leaves a laptop open and unlocked with an unattended patient while running for a medicine

sample. What should be done first?>

a. Nothing, the patient is trustworthy and a long-time customer
b. Immediately do a network security check and run an audit trail report to determine if any PHI was inappropriately accessed
c. Chastise the nurse about HIPAA security
b. Alert the HHS Office for Civil Rights of a breach>

7. What is considered inappropriate access of patient's PHI?>

a. Use information in order to treat a patient
b. Utilize PHI to bill for services provided to a patient
c. Review a friend's files after seeing her in the waiting area
d. Employ PHI to carry out job responsibilities>

8. If a state's privacy law is more "stringent" than HIPAA, which mandate is followed?>

a. HIPAA because federal rules always come first
b. The state's law would preempt the HIPAA Privacy Rule
c. Neither>

9. If a breach impacts less than 500 individuals, the covered entity _____.>

a. Doesn't have to notify anyone
b. Must notify the media
c. Must notify the HHS Secretary within 60 days
d. Must pay a fine immediately to the HHS Office for Civil Rights>

10. According to the HIPAA Security Rule, risk analysis and management include:>

a. Regular evaluations concerning the risks to ePHI
b. Adoption and implementation of safeguards to circumvent risks to ePHI
c. Appropriate updates that ensure the security measures are being met
d. All of the above>

Answers: 1) D; 2) D; 3) B 4) B; 5) C; 6) B; 7) C; 8) B; 9) C; 10) D. >