Health Information Compliance Alert

Security Rule Quiz: Security 101: Do You Know The Basics Of HIPAA's Security Rule?

From password functions to server vulnerabilities, conference attendees at the most recent HIPAA Summit in Baltimore were polled to determine their security rule awareness. Although there could be more than one correct answer to some questions, **John Parmigiani**, National Practice Director, **CTG HealthCare Solutions, Inc.** and moderator for this particular session of the summit, tells **Eli** that there are "preferred" answers - answers that each panel member agreed to be correct - for each question.

Question 1. The primary function of a password is to:

a. Permit access to pro grams and files
b. Identify the user
c. Authenticate the user
d. Authorize the user
e. Frustrate doctors

Question 2. Passwords should be changed every ...

a. 30 days
b. 60 days
c. 90 days
d. 180 days
e. At least once a year

Question 3. Which of the following password management methods would you consider to be the weakest practice?

a. Change passwords at least once a year
b. Have users select their own passwords
c. Use a minimum length of seven alpha-numeric characters
d. Periodically run a password crack program

Question 4. E-mail containing ePHI can be sent over the Internet.

a. No
b. Yes
c. Yes, if the e-mail is encrypted
d. Yes, if the covered entity conducted a risk analysis and determined it is okay to send ePHI by e-mail
e. I'm not sure and that's why I'm here

Question 5. The person who has been designated with the responsibility for security (Information Security Officer) should report:

a. At a level equal to the CIO
b. To the CIO
c. To Internal Audit
d. To Corporate Compliance

e. To any department except IT

Question 6. The most effective control for diminishing the risk of electronic media based disclosure of data is to:

a. Ensure that floppy disks are write protected when not in use
b. Require every file be individually encrypted when not in use
c. Disable or remove floppy drives and CD-ROM writer drives
d. Mandate that people caught using floppy disks receive a verbal warning

Question 7. The greatest vulnerability to servers that process and store sensitive and/or ePHI is:

a. Servers are not properly configured
b. Too many users have generic logons
c. Audit trails are not being used
d. The variations of hardware and operating systems make it difficult to maintain an accurate inventory of systems.

Question 8. The majority of security incidents are caused by:

a. Intentional outsider actions
b. Unintentional outsider actions
c. Intentional employee actions
d. Unintentional employee actions.

ANSWERS:

1) C 2) D

3) B 4) D

5) D 6) B

7) A 8) D