Medical Identity Theft

Deadline: Postmarked no later than September 1, 2024
Credit: 2.5 AAMA CEUs (gen/admin) Code: 143134
Directions: Determine the correct answer to each of the following, based on information derived from the article.

Electronic bonus! This test is available on the e-Learning Center at learning.aama-ntl.org. Miss the postmark deadline? Take the test online instead!

T F 1. Medical identity theft and medical identity fraud are interchangeable terms that can be used to describe the same conduct.

T F 2. More than 700 large health care data breaches occurred in the United States in 2023, according to the U.S. Office for Civil Rights.

T F 3. Medical identity theft is easily and quickly detected, and the victim's resulting loss is limited.

T F 4. A data breach in patient health information can result in illegal access to financial information and theft.

T F 5. Medical identity theft represents a large percentage of identity theft.

T F 6. Two-factor authentication requires a user to provide two forms of identification to access an online account.

T F 7. Medical identity fraud is defined as the actual misuse of data to obtain medical care, durable medical equipment, and prescriptions.

T F 8. Medical information theft is primarily a problem for large health systems and less of a problem for small provider practices.

T F 9. Because of recent federal legislation, a central repository of medical records is used so that victims of medical identity theft and fraud can quickly identify the extent of the criminal use of their information.

T F 10. A drop in a person's credit score for no apparent reason can indicate medical identity theft.

T F 11. Health care information ranks behind Social Security numbers and credit card information as the most sought-after information by criminals.

T F 12. Cybersecurity is more effective for health care organizations than for other sectors of the economy.

T F 13. Medical identity theft can result in incorrect information being entered into a patient's health record.

T F 14. Health care delivery settings should have a protocol for reporting medical identity theft to patients who have had their medical information stolen.

T F 15. Obtaining medical care in the name of a theft victim is an example of criminal use of patient health information.

T F 16. To protect confidential information, staff in medical practices and clinics should not click on links from email addresses they do not recognize.

T F 17. More than 30 states have adopted some form of comprehensive privacy and security law.

T F 18. To lessen the likelihood of unauthorized access to patient information, staff should carefully review and verify requests for the release of health information.

Take your learning online! Earn CEUs on the e-LC.

Take this course and more on the AAMA e-Learning Center and realize the benefits:
• Secure online payment
• Immediate test results via email
• Instant updates to your AAMA CEU transcript

Visit the e-LC at learning.aama-ntl.org