Mindful Continuing Education

Facilitating the Privacy and Security of Electronic Health Information

Chapter 1: Why Do Privacy and Security Matter?

1. Patients must trust the confidentiality and accuracy of their health records so they feel confident disclosing pertinent health information and to enable better informed decisions.

A. True
B. False

---

2. The professional practice itself and the Electronic Health Record (EHR) developer must share equal responsibility in taking the steps needed to protect the confidentiality, integrity and availability of health information.

A. True
B. False

What Types of Information Does HIPAA Protect?

3. The Privacy Rule protects most individually identifiable health information held or transmitted by a covered entity (CE) and its business associates (BA), and it includes demographic information that relates to each of the following EXCEPT:

A. The individual's past, present, or future physical or mental health or condition
B. The provision of health care to the individual
C. General health care plans that include average information of the group
D. The past, present, or future payment for the provision of health care to the individual

---

The HIPAA Privacy Rule

4. The Privacy Rule establishes national standards for the protection of certain health information and addresses the use and disclosure of PHI as well as standards for individuals' privacy rights to:

A. Understand and control how their health information is used and shared
B. Examine and obtain a copy of their health records
C. Request corrections of records

D. All of the above

Do I Have to Get My Patients' Permission to Use or Disclose Their Health Information with Another Health Care Provider, Health Plan or Business Associate?

5. Except for disclosures to other health care providers for treatment purposes, professionals must make reasonable efforts to use or disclose only the minimum amount PHI needed for the purpose of the use or disclosure, which is called the "basic essential guideline".

A. True
B. False

6. In health care facilities where a directory of patient contact information is maintained, a CE may rely on an individual's informal permission to list in its directory the individual's name, religions affiliation, location in the facility and:

A. The patient's general condition
B. Insurance and other financial considerations
C. The specific treatment plan
D. The patient's emergency contact information

What is De-Identified PHI?

7. Once personal health information (PHI) is de-identified in accordance with the Privacy Rule, it is no longer PHI and thus may be used and disclosed by your practice or your BA for any purpose.

A. True
B. False

Chapter 3: Understanding Patients' Health Information Rights-Patient Access to Information

8. Patients have the right to inspect and receive a copy of their PHI in a designated record set, which includes information about them in your medical and billing records, and generally, a CE must grant or deny the request for access within 90 days of receipt of the request.

A. True
B. False

Rights to Restrict Information

9. Which of the following is NOT one of the circumstances in which individuals have the right to request restrictions of information?

A. Certain uses and disclosures of PHI for treatment, payment, and health care operations
B. Certain disclosures to persons involved in the individual's health care or payment for health care
C. Certain disclosures to law enforcement or court representatives about the individual's health history
D. Certain disclosures to notify family members or others about the individual's general condition, location, or death

---

Chapter 4: Understanding Electronic Health Records, the HIPAA Security Rule, and Cybersecurity

10. The HIPPA security rule includes administrative safeguards such as actions, policies, and procedures to prevent, detect, contain, and correct security violations, to protect electronic PHI, and to manage the conduct of workforce members in relation to the protection of that information.

A. True
B. False

Working with Your EHR and Health IT Developers

11. When working with your EHR and health information technology (health IT) developers, important questions should be, 'When my staff is trying to communicate with the health IT developer's staff, how will each party authenticate its identity?' and "How much remote access will the health IT developer have to my system to provide support and other services and how will this remote access be secured?"

A. True
B. False

Email and Texting

12. The Security Rule requires that when a provider sends ePHI to a patient, it is sent through a secure method and that that there a reasonable belief that it will be delivered to the intended recipient, and that the provider ensures that the patient is sending health information that is secure before accepting such correspondence.

A. True
B. False

Chapter 5: Medicare and Medicaid EHR Incentive Programs Meaningful Use Core Objectives that Address Privacy and Security-General Overview

13. Stage 1 Meaningful use criteria focuses on using that information to track key clinical conditions and communicating that information for care coordination purposes, implementing clinical decision support tools to facilitate disease and medication management, using EHRs to engage patients and families, reporting clinical quality measures and public health information, and:

A. Encouraging the use of health information technology health IT
B. Electronically capturing health information in a structured format
C. Quality improvement at the point of care
D. Exchange of information in the most comprehensive format possible

---

14. .Examples of Stage 2 meaningful use include the electronic transmission of orders entered using Computer Provider Order Entry (CPOE) and the electronic transmission of diagnostic test results.

A. True
B. False

Chapter 6: Sample Seven-Step Approach for Implementing a Security Management Process

15. The security management process standard is a requirement in the HIPAA Security Rule, and conducting a risk analysis is one of the requirements that provides instructions to implement the security management process standard.

A. True
B. False

Sample Seven-Step Approach for Implementing a Security Management Process

16. When implementing a security management process, likely steps will include each of the following EXCEPT:

A. Lead your culture, select your team, and document your process, findings, and actions
B. Review existing security of ePHI, develop an action plan, and manage and mitigate risks

C. Attest for meaningful use security-related objective and monitor, audit, and update/security on an ongoing basis
D. Inform patients and clients of the nature of any security threats and actions to deter such threats

---

Tips For A Better Security Risk Analysis

17. In order to enable a successful security risk analysis, it is helpful to educate staff about the ongoing nature of the process and make security a high priority in the workplace culture.

A. True
B. False

Step 5A: Implement Your Action Plan

18. The goal of following your security risk action plan is to protect patient ePHI through ongoing efforts to identify, assess, and manage risks, and the plan should address clinical, patient and enforcement safeguards.

A. True
B. False

Medical Record Retention

19. State law requires providers to store medical records for a specified number of years, and obligations and the length of time to maintain patient medical records recorded in an EHR are usually also a matter of the stateâ€™s medical record retention laws.

A. True
B. False

Chapter 7: Breach Notification, HIPAA Enforcement, and Other Laws and Requirements

20. Under HIPAA, the U.S. Department of Justice can impose criminal penalties for knowing misuse of unique health identifiers and knowing and unpermitted acquisition or disclosure of Protected Health Information.

A. True
B. False

Risk Assessment Process for Breaches

21. Which of the following is NOT one of the minimum required elements when conducting a risk assessment to determine if a breech has occurred?

A. The nature and extent of the PHI involved in the use or disclosure, including the types of identifiers and the likelihood that PHI could be re-identified
B. The unauthorized person who used the PHI or to whom the disclosure was made
C. The likelihood that any PHI was actually acquired or viewed and the extent to which the risk to the PHI has been mitigated
D. The level of reasonable vigor or earnestness to protect information that occurred at the time of the disclosure

---

Investigation and Enforcement of Potential HIPAA Rules Violations

22. In general, The HIPAA Enforcement Rule provides different penalties for violations due to "unintentional neglect" that are corrected within 60 days and those due to "unintentional neglect" that are not corrected within 60 days.

A. True
B. False
