

HIPAA PRIVACY & SECURITY RULE PROFICIENCY EXAM

Test your organizations HIPAA knowledge – the answer key is provided at the end.
(Don't peek at the answers – you're only hurting yourself and your practice)

1. Which of the following uses of patient health information do not require the patient's authorization?
 - a. Treatment, payment, health care administration
 - b. Marketing
 - c. Genetic testing and research studies
 - d. Release of psychotherapy notes

2. Which of the following are considered protected health information under HIPAA? Select all that apply.
 - a. Phone number
 - b. Medical record number
 - c. License plate number
 - d. Email address

3. HIPAA rules do not require providers to grant patient access to which of the following types of information?
 - a. Accounting disclosures
 - b. Office visit documentation
 - c. Psychotherapy notes
 - d. Medication list

4. The "Notice of Privacy Practices" explains the ways the practice will use patient information and describes patients' rights regarding their information.
 - a. True
 - b. False

5. There are three things that a practice must do regarding communicating with the patient about privacy practices and procedures, except for one of the following:
 - a. Give every patient a notice describing the physician office privacy practices
 - b. Make a "good faith" effort to obtain the patient's written acknowledgment of receiving the notice
 - c. Obtain the patient's authorization for disclosures or uses not covered by the "Notice of Privacy Practices"
 - d. Give every patient a copy of his or her medical record

6. Sign-in sheets include protected health information. However, they may be used without violating privacy rules for this reason:
- Patient name is not protected health information
 - The sign-in sheet is used for health care operations and is considered an incidental disclosure
 - The patient name is usually not legible
 - Not all persons signing the sheet are patients
7. A physician office employee sees her neighbor at the office. It is acceptable for the employee to mention to another friend that she saw the patient at the doctor's office, as long as the employee did not mention why the patient was there.
- True
 - False
8. The rights of individual patients under HIPAA rules cover their access to their information and its disclosure to others. Which of the following is not a patient right under HIPAA rules?
- To inspect and copy his or her health information
 - To request changes to his or her records
 - To obtain an accounting of disclosures of his or her information
 - To inspect the protected health information of his or her spouse
9. When must the patient authorize the use or disclosure of health information?
- At every visit
 - Only when the information will be provided to law enforcement
 - Only when used for purposes other than treatment, day-to-day operations, or to comply with a request to which the practice is legally obligated to respond
 - Only in emergency situations
10. HIPAA rules and regulations cover what kind of information?
- All personal health information in any format, for any person
 - Protected health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral
 - Diagnoses and procedure information
 - All health information for persons who have insurance
11. Under what circumstances are employees allowed to repeat to others PHI that is heard or seen on the job?
- Only when authorized for their job duties
 - Once they have been terminated
 - After a patient dies
 - If they do not think the patient would mind

12. What should an employee do when he or she suspects another employee is in violation of the privacy or security policies?
- Gather solid evidence against the person
 - Confront the individual and tell the person that he or she is violating the rules
 - Nothing
 - Report suspicions to the office manager, privacy/security officer, or other designated person
13. Which of the following phrases should employees keep in mind when deciding if they should access a patient's information?
- Since the employee works there he or she can access every patient's information
 - Just a quick peek at a file will not hurt anything
 - Only use what is needed to perform his or her job duties
 - Thinking it is okay to look at a patient's information as long as it is not shared with anyone else
14. A staff member needs to leave a HIPAA compliant message on a voicemail or with someone else. Which of the following is not an acceptable practice when contacting patients via phone?
- Following the minimum necessary standard when leaving a message with whoever answers the phone
 - Leaving detailed PHI on a voicemail without having the patient's permission
 - Leaving the minimum amount of information needed: name, number, and practice or physician name
 - Leaving a detailed message, if the patient has given permission to do so
15. One of the administrative safeguard standards under the Security Rule deals with information access management. One of the basic rules of access management is:
- Information users should be authorized to access only the information they need to do their jobs
 - Information users should never be allowed to discuss protected health information
 - Patients are routinely questioned about their need to access medical records
 - Only clinical personnel should have access to medical records
16. Workstation security is among the physical safeguard standards. Which item below is not an appropriate practice?
- Workstations placed in a physically secure location
 - Visitors should not be able to view information on computer screens
 - Administrator workstations that can enable or disable security features located in secure areas
 - Computer stations located in a patient waiting room

17. Before faxing PHI or confidential information, which of the following should an employee do? Select all that apply.
- Use a fax cover sheet with approved confidentiality statement
 - Confirm the fax number before sending
 - Send the minimum information necessary
 - Use any cover sheet as long as it contains the organization's name and contact information
18. The HIPAA security regulations apply only to protected health information in electronic form. What about the HIPAA privacy regulations?
- These also apply only to information in electronic form
 - Privacy regulations apply to information being faxed
 - Privacy regulations do not apply to Medicare patients
 - Privacy regulations apply to both paper and electronic formatted information
19. Why is giving away old computer equipment used by a health care provider's office more of a security risk than just placing the equipment in the trash?
- Recipients of old computer equipment will ultimately destroy the equipment
 - PHI may remain on the equipment
 - Equipment may contain blood-borne pathogen contamination
 - Once given away, the equipment cannot be tracked
20. What is the definition of a breach of protected health information?
- Access, use, or disclosure of PHI that compromises security or privacy of the PHI
 - Inadvertent release of clinical information
 - An incident in which PHI leaves the physician practice
 - Theft of any equipment from a physician office or hospital
21. A physician employee is working at a satellite office on Tuesday. On Monday, he takes a laptop home so he can go straight to the satellite office the next morning. What is the best practice to secure the laptop overnight?
- Lock it in the trunk of the car
 - Cover it up with something and lock it inside the car
 - Leave it in the car, but pull inside the garage
 - Take it inside and keep it in a secure location
22. When using email to communicate with patient, what method out of the following is an appropriate safeguard per the Security Rule guidelines?
- Asking the patient to delete the message immediately after he or she reads it
 - If a patient emails the employee first, the Rule does not apply
 - Using encryption to send the email to the patient
 - Only using patient's medical record number in the email not his or her name

HIPAA PRIVACY & SECURITY RULE PROFICIENCY EXAM – ANSWER KEY

<p>Question 1: a. Treatment, payment, health care administration</p>	<p>Question 2: a. Phone number b. Medical record number c. License plate number d. Email address</p>	<p>Question 3: a. Psychotherapy notes</p>	<p>Question 4: a. True</p>
<p>Question 5: a. Give every patient a copy of his or her medical record</p>	<p>Question 6: a. The sign-in sheet is used for health care operations and is considered an incidental disclosure</p>	<p>Question 7: a. False</p>	<p>Question 8: a. To inspect the protected health information of his or her spouse</p>
<p>Question 9: a. Only when used for purposes other than treatment, day-to-day operations, or to comply with a request to which the practice is legally obligated to respond</p>	<p>Question 10: a. Protected health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral</p>	<p>Question 11: a. Only when authorized for their job duties</p>	<p>Question 12: a. Report suspicions to the office manager, privacy/security officer, or other designated person</p>
<p>Question 13: a. Only use what is needed to perform his or her job duties</p>	<p>Question 14: a. Leaving detailed PHI on a voicemail without having the patient's permission</p>	<p>Question 15: a. Information users should be authorized to access only the information they need to do their jobs</p>	<p>Question 16: a. Computer stations located in a patient waiting room</p>
<p>Question 17: a. Use a fax cover sheet with approved confidentiality statement b. Confirm the fax number before sending c. Send the minimum information necessary</p>	<p>Question 18: a. Privacy regulations apply to both paper and electronic formatted information</p>	<p>Question 19: a. PHI may remain on the equipment</p>	<p>Question 20: a. Access, use, or disclosure of PHI that compromises security or privacy of the PHI</p>
<p>Question 21: a. Take it inside and keep it in a secure location</p>	<p>Question: 22: a. Using encryption to send the email to the patient</p>		