HIPAA PRIVACY & SECURITY - HITECH TRAINING QUIZ

NAME _____ DATE _____

PART I – HIPAA PRIVACY TRAINING

INSTRUCTIONS: Circle the letter of the **most correct** answer.

1. What does "HIPAA" stand for?
- a) Health Insurance Portability and Accountability Act
- b) Healthcare Industry Privacy and Accountability Act
- c) Health Insurance Privacy and Administration Act
- d) None of the above

2. What is PHI (Protected Health Information)?
- a) Covered transactions (eligibility, enrollment, health care claims, payment, etc,) performed electronically.
- b) Information about past or present mental or physical condition of a patient.
- c) Information that can be used to identify a patient.
- d) All of the above.

3. What does HIPAA do?
- a) Protects the privacy and security of a patient's health information.
- b) Provides for electronic and physical security of a patient's health information.
- c) Prevents health care fraud and abuse.
- d) All of the above.

4. I can be disciplined for posting information about patients on any social networking site.
- a) True
- b) False

5. When can you use or disclose PHI?
- a) For the treatment of a patient, if that is part of my job.
- b) For obtaining payment for services, if that is part of my job.
- c) When the patient has authorized, in writing, its release.
- d) All of the above.

6. How does a patient learn about privacy under HIPAA?
- a) They look it up on the internet.
- b) They ask the dentist or the office manager.
- c) At their first visit they are given the Provider's Notice of Privacy Practices, and signs an acknowledgement that they have received a copy of it.
- d) The Government sent this out in the mail to every U.S. Citizen prior to April 14, 2003.

7. Who at your dental office has to follow HIPAA Law?
- a) Every employee.
- b) Dentists at your dental office.
- c) Employees who provide management, administrative, financial, legal, or operational support to your dental office, if they use or disclose individually identifiable Health Information.
- d) b) **and** c).

8. May you fax a patient's Protected Health Information?

a) Yes, if you use a cover sheet containing a Confidentiality Statement and you verify the number with the recipient prior to sending the fax.
b) Faxing PHI is never appropriate.

9. Looking up a co-worker or family member's personal health information is okay.

a) True
b) False

10. Dentists can have access to any patient's record or information, even if they are not treating the patient.

a) True
b) False

11. Which of the following releases must be logged in an "Accounting of Disclosures Log?"

a) Releases the patient has authorized.
b) Releases for payment, treatment, or operations purposes.
c) Accidental releases, legal releases (subpoenas, etc.)

12. Which of the following is NOT an example of false claims?

a) Overcharging for a product or service.
b) Billing for a service that was provided.
c) Billing for a service that was not medically necessary.
d) Billing for a different service than what was actually done to 'give the patient a financial break'.

13. If a police officer comes in and demands a patient's chart, you should:

a) Give it to the officer immediately but make him read it there.
b) Tell the officer you can't find the chart and delay until he gets tired of waiting.
c) Make a copy of the subpoena, search warrant, etc. Then, ask the officer to take a seat, and then fax the information to legal counsel or the Compliance Officer. Wait for further instructions from legal or compliance.

14. Which of the following is NOT an approved way to dispose of Personal Health Information (PHI)?

a) Shredder Bin or cross-cut shredder.
b) Regular trash after marking out PHI with black indelible marker.
c) Red biohazard bags.

15. Patients can look at their own charts whenever they want.

a) True
b) False

16. It is best to ask the patient's permission every time before discussing anything in the presence of visitors or family members.

a) True
b) False

17. Personal Health Information (PHI) is often misused. Which of the following is an example of misuse?

a) Payment of an insurance claim.
b) Treatment purposes.
c) Celebrity snooping.

PART 2 – HIPAA SECURITY TRAINING

18. A co-worker is called away for a short errand and leaves the clinic PC logged onto the confidential information system. You need to look up information using the same computer. What should you do?

a) Log your co-worker off and re-log in under your own User-ID and password.
b) To save time, just continue working under your co-worker's User-ID.
c) Wait for the co-worker to return before disconnecting him/her; or take a long break until the co-worker returns.
d) Find a different computer to use.
e) a) **and/or** d)

19. Which workstation security safeguards are YOU responsible for using and/or protecting?

a) User ID
b) Password
c) Log-off programs
d) Lock up the office or work area (doors, windows, laptops)
e) All of the above

20. To guard against unauthorized access to electronic Protected Health Information (ePHI) that being sent via email, you must encrypt the message and any attachments containing PHI or confidential information.

a) True
b) False

21. Which of the following statements is NOT correct about securing your workstation?

a) You must take all necessary precautions.
b) Secure the workstation when walking away.
c) Log-off at the end of the day.
d) Ask your co-worker to watch over your computer when you are not there.

22. It is okay to tape your password to your computer as long as you put it on the side, where it is out of sight.

a) True
b) False

23. You should never let anyone access a computer under your log-in.

a) True
b) False

Part 3 – HITECH TRAINING

24. The Final Omnibus Rule (HIPAA and HITECH), defines a breach as:

a) Any unauthorized acquisition, access, use, or disclosure of protected health information in a manner not otherwise permitted under HIPAA.
b) The unintentional acquisition of or inadvertent disclosure of PHI from one person authorized to access PHI to another
c) a place for fun in the sun.

25. Unsecured protected information can include information in any form or medium, including electronic, paper, or oral form.

a) True
b) False

26. It is acceptable to wait to report a breach of PHI until you return from vacation if you discover one right before you leave.

a) True
b) False

27. Who should a breach be reported to?

a) Co -workers
b) Your supervisor, the HIPAA Compliance Officer, or Attorney for your dental practice
c) The dentist
d) The hygienist

28. Which of the following is an exception to a breach?

a) Discharge papers being given to the wrong patient
b) Files stolen from a workspace
c) A billing employee reading and retaining an e-mail not intended for him/her and discusses the detailed information with others
d) An EOB sent to the wrong patient and returned as undeliverable

29. A breach is considered discovered

a) when the incident becomes known.
b) when it occurs.
c) when the covered entity or Business Associate concludes the analysis of whether the facts constitute a Breach.
d) when the affected individual finds his/her identity stolen.

Part 4 – HB300 TRAINING

INSTRUCTIONS: Circle the letter of the **most correct** answer

30. Written requests for access to or copy of Protected Health Information must be fulfilled within:

a) 30 business days
b) 15 business days
c) 30 calendar days
d) 15 calendar days

31. A "Covered Entity" is:

a) An organization that, for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information.
b) An organization that possesses PHI
c) An organization that obtains or stores PHI
d) All of the above

32. Each covered entity shall provide training to employees of the covered entity regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out the employees' duties for the covered entity.

a) Within 60 days of hire date and every 2 years
b) Within 60 days of hire and as changes in the law occur
c) Within 90 days of hire date and every 2 years
d) Within 90 days of hire and as changes in the law occur