Annual HIPAA Training Quiz
(For Medical Clinic Staff – Privacy, Security, and Compliance Review)

- 80% or higher (16 correct answers out of 20) is recommended for compliance confirmation.
- Staff who score below 80% should review missed items and complete a short refresher with the Privacy Officer before retaking the quiz.

Instructions: *Circle or mark the best answer for each question. Some may have more than one correct answer.*

---

1. HIPAA stands for:
A. Health Insurance Portability and Accountability Act
B. Health Information Privacy and Accountability Act
C. Health Industry Protection and Access Act
D. Health Information Portability and Access Agreement

---

2. The purpose of HIPAA is to:
A. Protect patient privacy and secure health information
B. Regulate hospital construction standards
C. Establish medical billing codes
D. Allow sharing of information freely between providers

---

3. PHI (Protected Health Information) includes:
A. A patient's name and date of birth
B. Medical record numbers
C. Photographs of a patient's face
D. All of the above

---

4. Which of the following is an example of a HIPAA violation?
A. Discussing a patient case in the cafeteria
B. Emailing PHI using unencrypted email
C. Leaving patient charts unattended at the front desk
D. All of the above

---

5. The “Minimum Necessary Rule” means:
A. Only share the least amount of PHI needed to perform your job duties
B. You can share PHI freely with coworkers
C. All staff can access full patient charts
D. PHI can be shared with anyone asking for it

---

6. When sending PHI electronically, you must:
A. Use encryption or an approved secure messaging system
B. Use your personal email account for convenience
C. Attach it to a text message
D. Copy yourself on every email

---

7. If you suspect a breach or accidental disclosure of PHI, you should:
A. Report it immediately to the Privacy/Security Officer
B. Ignore it if it seems small
C. Try to fix it yourself before telling anyone
D. Delete the email and move on

---

8. Which of the following is *not* considered PHI?
A. Social Security Number
B. Email address linked to a patient
C. Weather report
D. Patient phone number

---

9. Employees are responsible for protecting PHI:
A. Only when the Privacy Officer is present
B. Only during work hours
C. At all times, including when working remotely
D. Only when handling paper records

---

10. A strong password should:
A. Be short and easy to remember
B. Include a mix of letters, numbers, and symbols

C. Be the same across all systems for simplicity
D. Include personal info like your birthday

---

11. Which of the following could be a phishing attempt?
A. An unexpected email asking you to click a link to verify your login
B. A message from IT with proper clinic contact info and internal address
C. A system alert from your computer's antivirus program
D. A password reset you personally requested

---

12. If you see a coworker accessing a chart for a patient they're not treating, you should:
A. Ignore it; they might have a reason
B. Politely remind them of HIPAA and/or report to a supervisor
C. Post about it on social media
D. Confront the patient directly

---

13. Paper PHI should be disposed of by:
A. Throwing it in the trash
B. Shredding or placing it in designated shred bins
C. Saving it for later in your locker
D. Taking it home to review

---

14. Which of these requires patient authorization before disclosure?
A. Sharing records for treatment between providers
B. Providing information for payment or insurance claims
C. Disclosing information to a family member not listed as an approved contact
D. Using PHI for internal quality improvement

---

15. HIPAA violations can result in:
A. Disciplinary action or termination
B. Civil or criminal penalties
C. Fines for the organization
D. All of the above

---

16. If a device containing ePHI (like a laptop or tablet) is lost or stolen, you should:
A. Immediately report it to your supervisor or Privacy Officer
B. Wait a few days to see if it turns up
C. Try to access patient data remotely before reporting
D. Post a lost-and-found ad online

---

17. When discussing patient information with another staff member:
A. Ensure the conversation is private and relevant to patient care
B. It's fine anywhere as long as no patients are listening
C. It's fine in elevators or hallways
D. None of the above

---

18. True or False: HIPAA only applies to electronic records.
A. True
B. False

---

19. True or False: Patients have the right to request corrections to their medical record.
A. True
B. False

---

20. True or False: It's acceptable to share your login with a coworker if they need quick access.
A. True
B. False

Employee Acknowledgment:
I have completed this HIPAA training quiz and understand that protecting patient privacy and data security is part of my job responsibility.

Name: _____ **Date:** _____

Signature: _____