Name _____ Date of Exam _____ Score _____

Confidentiality
Written Competency

TRUE FALSE 1. HIPAA and the code of federal regulation (42CFR, Part 2) refer to exactly the same rules governing client privacy.

TRUE FALSE 2. HIPAA provides guidance to the health care community in relation to patient information and privacy.

TRUE FALSE 3. HIPAA only addresses written health records, and does not apply to client records stored or shared through Electronic Data Interchange.

TRUE FALSE 4. Once information is entered into WITS it is considered safe and protected, so sharing passwords among staff inside your agency is acceptable.

TRUE FALSE 5. If a person has the ability to access facility or organization systems or applications, they have a right to view any information contained in that system or application.

TRUE FALSE 6. An individual's participation in ATR Ohana is considered protected health information.

TRUE FALSE 7. Discussions about clients or client information in public areas, such as the cafeteria, may be overheard by unauthorized listeners and may violate the client's right to privacy.

TRUE FALSE 8. Acknowledging a client in public may violate confidentiality. Providers and clients should discuss this possibility and make a plan for how to react in such a situation.

TRUE FALSE 9. The Privacy Act limits the collection of information about individuals to that which is relevant and necessary.

TRUE FALSE 10. Clients, for the most part, may gain access to any information pertaining to them that is contained in any system of records.

TRUE FALSE 11. If the client wants access to their record, they must provide in writing a valid reason for wanting to see their record.

TRUE FALSE 12. Signed authorizations for release of information are considered invalid if there is not an expiration date.

TRUE FALSE 13. Disclosure of substance abuse information to an outside healthcare provider even for treatment purposes requires a written authorization by the client.

Name _____ Date of Exam _____ Score _____

TRUE FALSE 14. All ATR Ohana staff (staff, providers, students, volunteers and contractors) are responsible for compliance with confidentiality laws and rules, including HIPAA Privacy Rules compliance, and must report concerns when noted.

TRUE FALSE 15. Protected health information is individually identifiable health information in any form (paper, electronic, oral) that is transmitted and/or stored by a covered entity or business associate.

16. What does HIPAA stand for?
    a. Health Information Privacy And Access
    b. Health Insurance Portability and Accountability Act
    c. How Information is Protected to Address Access
    d. Have Information on Patient Addiction Available

17. When do you use Release of Confidential Information authorization forms?
    a. When a health care professional must disclose confidential substance abuse information to other health care professionals in other organizations.
    b. When client identifying data is entered into a third-party maintained data base.
    c. When billing substance abuse information is released to a third-party payer.
    d. When exchange of treatment information is used to coordinate client care.
    e. All of the above.
    f. Only a and d.

18. Where and how should client paper information be stored?
    a. In a file cabinet at the agency that is left open for convenience to all agency staff.
    b. In a locked file cabinet in a secure area that permit access to only essential agency staff.
    c. Turned upside down on the desk when left out overnight.
    d. Face up on the agency staff's desk as long as the door to that office is closed when no one is inside that office.
    e. All of the above are considered secure client record storage.

19. When do you use the Notice of Privacy Practices?
    a. ADAD requires the Notice of Privacy Practice to be issued to all clients, and to be signed by the client and by the staff providing the Notice.
    b. Only when the client's record may be released outside of the provider's agency.
    c. Only when the client asks about confidentiality practices of the agency.

20. Firewalls and passwords help to protect:
    a. Your agency's computer records from outside hackers.
    b. Electronic transmissions and e-mails.
    c. Individual computer tower contents from other staff in your agency.
    d. All of the above.
    e. Only a and b.

Name _____ Date of Exam _____ Score _____

21. The criminal penalties for improperly disclosing client health information can be as high as:
    a. Fines of $5,000 and jail sentences of up to 12 months.
    b. Fines of $250,000 and prison sentences of up to 10 years.
    c. Fines of up to $1,000,000 and prison sentences of up to 35 years.
    d. There are no criminal penalties for violating confidential client information; however, your agency may be liable in civil court for violations of HIPAA and 42 CFR, Part 2.

22. Confidentiality protections covers:
    a. Health-related information.
    b. Diagnosis.
    c. Social security number.
    d. Telephone numbers.
    e. Address.
    f. Record of attendance in treatment/recovery programs.
    g. All of the above.
    h. Only a and b.

23. You overhear a fellow staff telling someone over the phone about one of the clients that you work with. You believe the other person on the phone is the staff's sister. What do you do?
    a. Discuss your suspicions with another co-workers to decide whether to report the incident.
    b. Report your suspicions to your supervisor and/or ATR Ohana Program Director.
    c. Call the client anonymously to tell them about your suspicions.

24. You are logging into WITS on your computer first thing Monday morning. You enter your password but get a message that your log-in failed. You try again and it doesn't work. You are positive that you are using the correct password. What do you do?
    a. Notify the WITS Administrator so that they can research the problem.
    b. Wait for the system to clear itself.
    c. Ask your co-worker to let you use her log-on ID and password until the problem can be resolved.

25. PHI stands for:
    a. Personal Health Information.
    b. Protected Health Information.
    c. Private Health Information.
    d. Portable Health Information.

26. It is NOT appropriate to access a client's WITS record or hard copy file when:
    a. Billing for services provided to the client by another staff.
    b. The client is present.
    c. You notice your cousin sitting in the waiting room at your agency, and you are curious to find out why your cousin is there.
    d. All of the above.

Name _____ Date of Exam _____ Score _____

27. Unauthorized access is:
    a. Access/disclosure of information that an employee or provider does not have the job responsibility to access or share
    b. Prohibited and against 42 CFR, Part 2 and the HIPAA Privacy Rules
    c. Looking at another's provider's record when you are not involved in his/her care and do not have written authorization from him/her.
    d. All of the above.

28. Unauthorized access is accessing information for which you do not have a job responsibility to access or share. Protected health information that should be kept confidential includes a client's:
    a. Diagnosis, procedures received, lab results
    b. Name, address, and social security number
    c. Medical information stored electronically.
    d. All of the above.

29. You notice that someone has left a computer terminal unattended with the screen used to access client information in the WITS system on, and it appears that they are still logged in to the WITS system. The most appropriate action is:
    a. It is not your terminal, so you should leave it as is.
    b. Track down the staff and let them know what you discovered, and that next time you will report them to the supervisor.
    c. Do nothing until you think about the situation overnight and then discuss it with your co-worker the next morning.
    d. Log off the WITS system immediately and notify your supervisor what you found.

30. In the above situation, if you take no action and a client sitting near the terminal is able to look around in WITS and discovers the name of another individual in ATR Ohana, who is responsible for this breach of privacy?
    a. The client, since they should not have been snooping.
    b. The other staff, since they should not have left the terminal on and unattended.
    c. You, since you knew that a potential violation was reasonably possible.
    d. Your supervisor, since more training on confidentiality should have been provided.
    e. ADAD, since they are the host of the WITS system.
    f. No one, since accidents happen and no one had bad intentions.
    g. Only b, c, and d.