### NAME\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ DATE\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

###

### HIPAA Privacy and Security Awareness Quiz

**1.) Per HIPAA Law, the Colorado Department of Human Services (CDHS) is mandated to protect our clients against any reasonably anticipated threats or hazards to the physical and technical security and the integrity of their protected health information (PHI).**

To accomplish this mandate, what guidelines, policies and procedures has CDHS implemented?

1. Do not share access devices (badges, keys, combination codes). Wear your state ID badge, this helps to identify visitors.
2. Keep all portable computers, discs and memory locked up when not in use. Angle your computer away from public access.
3. Lock all desks, files, and doors as appropriate.
4. All of the above.

**2.)** **Individuals can be held personally responsible for failure to protect PHI.**

1. True
2. False

**3.) CDHS allows you to save PHI to your local C:/ drive?**

1. True
2. False

**4.) A new employee has just begun work.  They have not yet been assigned an account to log into the CDHS computer system.  Can you share your log in and password so they can begin work?**

1. No, your log in and password equals your signature. Do not share this information.
2. Yes you can share your password; it is not a big deal.
3. Maybe, ask your supervisor for approval.
4. Yes, sharing your log in and password will help the new employee to get started on their work assignments.

**5.) I agree to the following Confidentiality Statement:**

While performing my business duties, I may be given access to patient Protected Health Information whether in verbal, written or electronic format.

I will maintain in strictest confidence the Protected Health Information to which I have access. I will not share any confidential information with others who are not authorized, including other staff members, contractor, friends or family.  I will use my access to Protected Health Information for the sole purpose of conducting legitimate business of the Colorado Department of Human Services.

My access to patient Protected Health Information is often facilitated by electronic information systems. In the interest of maintaining the integrity of these systems and of ensuring the privacy, security and proper use of the State resources, I will not share my password to any such systems to which I have access.

I understand that the use of Protected Health Information, other than for legitimate business purposes, is strictly prohibited.

1. Agree
2. Disagree

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6.) Right to Request Accounting of Disclosures**

HIPAA gives individuals the right to an accounting of disclosures that we have made of their PHI for up to six years preceding the request.  Which of the following statements are true?

1. We are only obligated to account for disclosures made after April 14, 2003, which is the day the Privacy Rule became effective.
2. Because of this right, we must track all disclosures of PHI made by us or one of our business associates to other entities. Business associates must report all such disclosures to us as part of their contractual obligations.
3. The privacy notice explains how individuals can request such an accounting.
4. All of the above.

**7.) Which of the following is true about HIPAA?**

1. HIPAA protects the privacy of personal health information.
2. HIPAA gives individuals the right to see their own medical records.
3. HIPAA allows state laws that provide stronger privacy rights and access to stay in effect.
4. All of the above.

**8.) Protected Health Information (PHI) only refers to written documents inside an individual's medical record.**

1. True
2. False

**9.) A representative of a government agency asks to see an individual's medical records. You are not sure whether the disclosure would be proper under HIPAA.  What do you do?**

1. Ask the representative of the federal government whether his request complies with HIPAA.
2. Conduct research on the Internet.
3. Release the medical records as requested and then consult with the privacy officer to make sure you complied with HIPAA.
4. Ask your HIPAA Officer before releasing the information.

**10.) The CDHS HIPAA Sanction Policy states the following:**

1. Failure to comply with CDHS policies and guidelines will result in disciplinary action depending upon the type and severity of the violation.
2. It is contingent on whether it causes any liability or loss to the Department, and/or the presence of any repeated violation(s).
3. There is no requirement for advance notices, written or verbal warnings, or probationary periods.
4. All of the above.

**11.) When using a Flash Drive to store or copy confidential data, CDHS allows:**

1. Use of all flash drives.
2. ITS approved flash drive with hardware encryption and an enforced complex password.
3. Flash Drives are never permitted.
4. You may use a floppy disc but not a flash drive.

**12.) How do you properly dispose of confidential or Protected Health Information (PHI)?**

**NOTE:  This question refers to PHI that is not required to be retained for accounting disclosures.**

1. Place the documents in the regular trash bins.
2. Place it in a secured container designated for confidential disposal.
3. Store it in a cardboard box in your work area until you decide to dispose of it properly.
4. None of the above.

**13.) When can a staff person remove protected health information from a CDHS facility?**

1. When a staff person wants to work from home.
2. For personal use.
3. Never.
4. For official CDHS court purposes only. Examples: when transporting a patient to an outside treatment provider; Case Management working with clients off site; or as otherwise approved by individual Agency approved HIPAA policy and procedure.