ATTENTION:

You may have direct or incidental contact or access to Protected Health Information (PHI) on this assignment.

Please read the following materials carefully.

You will be quizzed on the information and you must pass the quiz to complete the onboarding process.

Thank you for your attention.

KFORCE℠

HIPAA and HITECH Training Guide

The **Health Insurance Portability and Accountability Act of 1996** (HIPAA) and **Health Information Technology for Economic and Clinical Health** (HITECH) are federal laws designed to safeguard **protected health information** (PHI). It is a requirement that anyone who has access to PHI take security training. You may receive or become aware of PHI on this assignment. Please review these training materials carefully. Failure to follow these may result in discipline up to and including termination of employment.

I. What is PHI and how should it be protected?

PHI means **any information** about status, provision, or payment for health care that can be **linked to a specific person** by many common identifiers such as:

- Name
- Social security number
- Address
- Date of birth
- Account or medical record numbers
- Email address
- Other identifiers

Some examples of health information include:

- Health insurance policy numbers
- Dates of treatment
- Any other pertinent information (medical history, condition, treatment, or diagnosis)

PHI must be protected at all times. This includes information found on:

- Computers
- Networks
- Paper
- Verbal information

Your obligations:

- Do not divulge, disclose, communicate, or use PHI except for a legitimate business purpose
- When using PHI, use only the minimum amount of the information required to complete a task
- Maintain PHI confidentiality not only throughout your employment, but also after your employment

Some examples of inappropriate uses and disclosures of PHI include, but are not limited to:

- Emailing PHI to a personal e-mail account or to unauthorized persons
- Transmitting PHI in an unsecured manner
- “Snooping” on PHI
- Downloading PHI to a phone, thumb drive, or other portable media for non-business purposes or when medium is not encrypted
- Leaving loose PHI paperwork unattended where it may be accessed by unauthorized persons
- Storing PHI in open network locations or on internet-based storage
- Selling PHI
- Disclosing PHI for purposes other than treatment, payment or health care operations

II. Where and how should PHI be stored and transmitted?

To the extent feasible, refrain from storing and transmitting PHI.

If you must store or transmit PHI to fulfill your job duties, make absolutely sure the information is kept **secure**:

- Store PHI in a location with limited access
- Encrypt PHI when it needs to be sent via email to someone outside Kforce or the client organization
- Lock up physical copies of PHI when not in use

The use of personal computers or devices to process, store, or access PHI **is strictly prohibited** without the prior approval of:

- The client, and
- The Kforce HIPAA Security Officer (HIPAASecurityOfficer@kforce.com)

Please keep in mind:

- Transport of PHI outside of a Kforce or client facility must be approved
- Transmitting PHI to or from a personal email accounts (i.e., Gmail, Yahoo, hotmail, etc.) is strictly prohibited
- Protect the security of anything that may give you access to PHI, such as passwords and keys

Best Practices for Protecting PHI

Do not film, photograph, or record audio in the workspace

Computers must employ a password protected screen saver

Enable the screen saver when leaving your computer unattended

Do not dispose of PHI unless authorized by the Kforce HIPAA Security Officer

Log off computers overnight or when leaving them unattended

Keep computers free of malicious software and viruses

Do not transmit PHI through a personal email address

III. What to do if you believe PHI has been improperly disclosed, transmitted, accessed, or stolen?

- Report all improper use, access, disclosure, or breach immediately to the Kforce HIPAA Security Officer at HIPAASecurityOfficer@Kforce.com

- **Immediate reporting of potential breaches is essential.** We may have a limited amount of time to respond to a potential breach. Response times are determined by:
  - Law
  - Client contracts
  - Our insurance policies

- Delays in reporting incidents can result in damage to Kforce's reputation and may have legal consequences

IV. What happens if you violate HIPAA?

Violations of the HIPAA and HITECH acts, as well client and Kforce policies may result in **disciplinary action**, up to and including **termination of employment**.

Additionally, **you can be held accountable** by federal and state authorities **for failure to comply** with applicable provisions of HIPAA and HITECH acts.

For additional information, refer to the full Kforce HIPAA and HITECH Policy located on the Kforce Consultant Website.

If you have questions about this training, please contact the Kforce HIPAA Security Officer at :

HIPAASecurityOfficer@kforce.com

Acknowledgement

I acknowledge that I have been made aware of the policy established by Kforce in accordance with the HIPAA and HITECH Acts which can be located on the consultant website (https://www.estaff365.com/account/login/).

As a Consultant of Kforce, I understand and certify that:

1. As a result of my assigned job duties, I may be granted access to systems which contain Protected Health Information (PHI).

2. I recognize the importance of maintaining the confidentiality and integrity of the PHI that I may come in contact with while performing my job duties.

3. I have reviewed the Kforce HIPAA and HITECH Training Guide.

4. I agree to abide by the Kforce HIPAA and HITECH Policy.

5. I understand that, by not following the Kforce HIPAA and HITECH Policy, I could be subject to disciplinary actions, including termination and that a violation of HIPAA and HITECH could result in civil or criminal penalties.

Sharp, Andrew B

Consultant Name (Print)

Digitally signed by Andrew B. Sharp
Location: andy@absharp.com
03/14/2022 06:13:39 PM -07:00

Consultant Signature

03/14/2022

Date