Privacy & Security Awareness

Privacy

Access to Protected Health Information by Job Role

In your current job role, you are allowed to access the electronic medical record (such as Lifetime Clinical Record), what do you need to know?

You should only access or disclose the information that is necessary to accomplish the specific task for your job.

Scenario:

A patient was last seen in your clinic in 2015 and you recently learn from the news media that the patient was involved in a shooting and admitted to ZSFG. Since he was your patient, how do you know when you are authorized to access his medical record?

Answer:

Even though the patient was last seen in your clinic, you are not authorize to access the patient’s medical record. Only access the patient’s medical record if you are part of the current treatment medical team.

Warning:

Accessing a patient’s medical record who you have previously treated and had since discharged or accessing a patient’s medical record out of curiosity or concern is considered an unauthorized access.

Violation for unauthorized access to a patient’s medical record will result in a privacy breach and may result in separation from your employment at ZSFG.

Security

How to prevent security threats?

Ways you can prevent phishing attempts, viruses, and spyware from accessing your computer and personal information:

- Do not respond to email requests or open attachments from unknown senders.
- Pause before clicking on any links or opening any attachments. If it looks suspicious, notify IT immediately.
- Phishing can also be over the phone, as the criminal callers are “phishing” for private information. Confirm the identity of the callers before providing private information. Secure all mobile devices and laptops with encryption.
- Keep your passwords secure. Do not share it with anyone.

Scenario:

You received an email from the HR department asking you to click on the HR link to provide your name, department, user login and password so that they can confirm your user account and update the directory. It states if you do not adhere to the notice, your account will be disable. What should you do?

Answer:

Do not respond and notify IT security immediately.

DPH IT: (628) 206-7378

Cyber criminals use links to direct users to their sites to collect your personal information or install malware on your computer system.

Helpful tip: When viewing links, place the mouse over the link without clicking on it and check where the link will direct you. Always ensure that the link is legitimate before clicking on it.

Report a Privacy Breach

Report every potential Breach of Protected Health Information (PHI):

- Your Local privacy Officer or
- Privacy Hotline: (855) 729-6040
- Email: compliance.privacy@sfdph.org
- Refer to Breach Reporting Form
- The Privacy Office also provides consultation on all privacy related questions. Please feel free to contact us.