Security Awareness in the Healthcare Setting

Understanding Threats

Your Responsibilities

Many employees don't realize the impact their actions have on the security of our organization and our patients. Whether you password protect your laptop or shred a confidential document, these seemingly minor decisions have a huge impact on information security.

Our number one defense against information theft and loss is you. Everyone is responsible for knowing and following our organization's security policies and procedures. By doing so, you ensure our information and resources remain secure, protect our reputation, and help us avoid costly penalties for violating the law.

Reporting an Incident

Just as you take steps to protect our information, you must also be sure to report any known incident involving threats to our information. An incident is any situation where protected information is lost, stolen, or otherwise improperly used. It could be anything from a stolen laptop to improperly shared payment card information, to a misaddressed e-mail containing sensitive information. If you witness an incident or even if a situation just doesn't seem right, you must act immediately and contact the appropriate person to investigate the incident. Remember, we rely on you to be mindful and trustworthy, and to follow our incident reporting procedures.

Physical Security Threats

Access Controls

Maintaining information security and protecting our facilities is one of our top priorities. The first step in protecting ourselves is understanding and avoiding actions that may put our physical security and information at risk. Tips to secure risks include: Keep your screen protected if in an area of that would allow view of any passerby; Do not allow anyone to enter the facility without proper identification; do not discuss patient information in any public setting where others may overhear; be attentive to personal devices so that they are not left unattended or left behind; do not leave paper charts or other PHI unattended and unsecured, including stepping away from station or desk.

Safe Computing

Phishing Threats

Phishing scams involve things like fake email designed by malicious hackers and thieves to look like it is coming from a trusted brand or institution – including your employer. Here are some ways to identify and avoid an attack: 1) Scams usually request urgent or immediate action within the subject line. 2) provide a link to click within the email.

WHAT YOU SHOULD DO:

1) Contact UH IST department to confirm suspicious email legitimacy.
2) Never click "Reply" to respond to questionable e-mails directly.

Password Guidelines

- Protect your userid and password. YOU are responsible for actions taken with you userid and password
- Do NOT post, write or share passwords with anyone.
- Use STRONG passwords that are hard to guess, easy to remember and change them often.
- Do NOT use a word from a dictionary - English or otherwise.
- Create a password between 8-10 characters (Upper- and lower-case letters, numbers, and special characters)
- Always Logoff/Disconnect from shared workstations.

Electronic Communications

If there is a need to send an e-mail that contains personal or sensitive information, the email must be encrypted.

If using data on a mobile devise. Ensure that your devise is set to password protected screen lock and use two-factor authentication whenever it is available.

When working remotely, outside Wi-fi networks pose a risk for data thieves to infiltrate. You should always use a virtual private network (VPN) connection to make good use of all protections of the UH network. Contact IST for information on how to enable VPN.

Protecting and Handling Date

Data Classifications: While some records contain information that is public knowledge, all protected health information must be guarded against unauthorized access. Our data classification and protection procedures help you understand what records need to be protected and what is available for public disclosure.

PUBLIC

Public information is available outside of our organization and is intended for public use. This includes patient information contained in the hospital directory (i.e., name, location, general condition).

There are few protection requirements for public data, but unless you are authorized to do so, never speak or release information on behalf of our organization.

INTERNAL USE ONLY

Internal data is information used by our organization for day-to-day processes and functions.

Internal data is not intended for public distribution and should be carefully managed and controlled.

CONFIDENTIAL

Confidential information includes important information about our employees and patients.

Confidential information is most often securely transmitted within our organization but requires stronger protection when shared outside of our network. Always check whether or not you are authorized to send confidential information before you share such information outside of our network.

RESTRICTED

Restricted data includes protected health information and is information that, if disclosed to unauthorized parties, could have serious legal repercussions and/or negative reputational consequences.

Restricted information requires the highest level of data protection.

Data Storage, Retention, and Destruction

It is necessary to know how to store protected health information, how long to retain it, and how and when to destroy it. The retention and destruction of patient, business, and other information is tied to both State and Federal law. Please access the UH Policies for information or consult with the Health Information Management Department, Compliance Department or Legal Department.

Data Transmission

Data transmission guidelines are designed to prevent unauthorized parties from accessing sensitive information. Access the UH Policies to ensure that sensitive information is not compromised during transmission. You can consult with the UH IST department for guidance to ensure proper protection of data transmission.