Health Information Portability Accountability Act (HIPAA)

In the Know

Health Information Portability Accountability Act, better known as HIPAA, is a federal law intended to protect consumer's health information. Over the past couple of years, new policies have been enforced and in which everyone should be familiar. HIPAA ensures the confidentiality, integrity and availability (CIA) of all electronic protected health information (PHI), protects against any "reasonably anticipated threats" and uses or disclosures that are not allowed by Privacy, and mitigates these threats by whatever safeguards you believe can "reasonably and appropriately" be implemented in line with Security rule standards. The Privacy Regulation is the intention of the regulation is to protect health information from non-medical uses by employers, marketers, etc.

HIPAA provides individuals with rights to

- Access to his/her records
- Request amendments to those records
- Receive an accounting of certain types of disclosures of health information
- Restrict the use of personal information. (i.e. The individual may request that SEARK not communicate with family members.)

To discuss any Protected Health Information, ***you must have authorization*** in order to disclose PHI; you must identify employees who may receive PHI; and you must divulge minimum necessary information. Authorization is required for any use or disclosure that is non-treatment, non-payment, or non-health care operations activity. (i.e. Authorization forms must be completed before HR can discuss any medical information with your insurance carrier, spouse or other family member.) Any entity that has the information must have authorization prior to disclosure. PHI also includes anything that any supervisor, manager or employee may see, hear or send. These forms can be obtained at http://www.arkansas.gov/dfa/employee_benefits/doc_rtf/authorization.doc Health information, including demographic data collected from an individual that is personally identifiable, is protected, such as:

- Permits identification of the individual or
- Could reasonably be used to identify that individual
- Examples: Name, Address, ID Number, Job Classification, Zip Code, Age, Job Tenure, Photo, Education Level, etc.

DO NOT ENGAGE IN ANY PRACTICES THAT YOU BELIEVE ARE A VIOLATION OF ANY REGULATION. If you believe you have encountered a privacy violation, you are required to act. Specifically, you may contact the supervisor, the Privacy Officer (or HR), or you may report the incident via the anonymous "hotline" at 1-800-TELLUSO.

Practical Applications:

1. ***A Mr. Smith calls in to talk to the supervisor who is not there and must talk to the admin assistant.*** It is the admin assistant's responsibility to keep that information confidential. *You must only disclose the minimum necessary information.*

2. ***Another supervisor comes to you and asks why Mr. Smith is not here***.....Again, only reveal the minimum necessary information. You are only allowed to say that that person is not in today.

3. ***A concerned supervisor wants to send his group an email about Mr. Smith in the hospital, this is his status, this is his situation***.....This cannot be done. You cannot release any information about the status of that employee without an authorization from that employee. If you do not have it in writing, you will be liable.

What happens when you are non-compliant?

- $100 each knowing failure to comply with a "provision", "prohibition", or requirement
- $25,000 annual cap on multiple violations of same "provision", "prohibition", or requirement
- Up to a One (1) year in jail

Southeast Arkansas College

1900 Hazel Street ◆ Pine Bluff, AR 71603
Website: www.seark.edu

HEALTH INSURANCE PROTIBILITY AND ACCOUNTIBILITY ACT (HIPPA)

Name: _____ Date: _____

1. Information that you acquire because of the position in which you were hired is private and should only be shared with other personnel on an as needed basis. Protected health information (PHI) received informally through conversation should be treated similarly, but since the information was given freely, it is less likely to be considered a breach under HIPAA. For example, if an employee calls in sick and gives you details to justify their absence, this should only be shared with other management as deemed necessary.
2. Efforts should be made to limits the release of personal information. Consider releasing the minimum information necessary at all times. For example, the reason someone is not at work is that they are sick; and take care not to disclose what is specifically wrong with them.
3. There should be an awareness of simple security measures in and around the office space. Information such as FMLA requests and doctor's excuses might contain protected health information (PHI) and should be locked up and/or covered when visitors are in your area.
4. Any paperwork containing protected identifiable information (PHI) should be shredded before being disposed of.
5. Under HIPAA, managers/supervisors are most at risk for HIPAA breaches. To protect yourself and your employees, everyone should be made aware of the policies.

I, the undersigned, understand and agree that the consequences of a violation of the above statements may result in disciplinary action up to and including termination as well as possible civil or criminal liability. I further understand that this document will be kept in my personnel file as proof of this discussion regarding my responsibilities with regards to HIPAA.

_____
Print Name

_____ _____
Signature Date