Human Resources 4U
hrexec@humanresources4u.com
(909) 912-9995

Health Insurance Portability and Accountability Act (HIPAA) Fact Sheet

What does HIPAA do?
HIPAA protects the privacy of medical records and personal health information (PHI)

Who is liable for PHI?
Health care providers, health plans, business associates, employers

What information is protected?
Information created or received by a health care provider, health plan, business associate, employer, etc., that relates to the past, present or future physical or mental health of an individual, the provision of health care to an individual or the payment for provision of health care to an individual

What is a Business Associate?
A "business associate" is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. Covered entities must have a written business associate contract or other arrangement with the business associate that establishes specifically what the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of protected health information.

When does HIPAA impact employers?

- When they need to obtain and use protected information
- If they administer their own health care plan or review health benefit decisions

What are some circumstances where an employer may need to obtain protected information?

- When obtaining medical information for FMLA purposes:
- To determine whether an employee has a serious medical condition
- To determine whether an employee is able to return to work
- When trying to determine the parameters of a reasonable accommodation under the ADA
- When trying to determine an appropriate modified work schedule for an employee returning to work after suffering a work-related injury

How may an employer obtain protected information?

The employer must obtain a valid authorization that includes the following:

- A description of the information
- The identity of the person/entity authorized to make the disclosure
- The identity of the person/entity to which the disclosure may be made
- A description of each purpose of the requested information
- The signature of the individual whose information is sought
- Certain statements notifying the individual of his or her rights, including that s/he is entitled to revoke the authorization and receive a copy of the requested information
- An expiration date

What are the potential penalties?

- Civil fines
    - Minimum fine is $100 per violation, maximum is $50,000 per violation
    - Maximum annual fine for multiple violations ranges from $25,000 to $1.5 million per violation
- Criminal fines
    - Up to $50,000 and one year in prison for disclosing protected health information
    - Up to $100,000 and 5 years in prison for obtaining protected health information under false pretenses
    - Up to $250,000 and 10 years in prison for obtaining or disclosing protected health information with the intent to use it for commercial advantage or malicious harm
- Imprisonment

Top HIPAA tips

- Keep all health information confidential and separate from other employee files
- Limit use of any protected information to those specifically provided in the authorization signed by the employee
- Request and use only the minimum amount of medical information necessary for your purpose