

HIPAA Cheat Sheet

What Does HIPAA Do?

The Health Insurance Portability and Accountability Act (HIPAA) protects the privacy of medical records and personal health information

What Information Is Protected?

Information created or received by a health care provider, health plan, 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

When Does HIPAA Impact Employers?

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

Note: Additional restrictions/obligations apply to health care plans and other health care-related entities under HIPAA

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 and criminal fines
- 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