Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established the national standards for the protection of health information that is held or transferred electronically. The Act has two components or rules - the Privacy Rule and the Security Rule.

The Privacy Rule establishes the national standards to protect individual's medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The Security Rule defines the technical and non-technical safeguards that "covered entities" (health care providers) must establish to secure health data. The Office for Civil Rights at the Department of Health and Human Services is responsible for enforcing the Privacy and Security Rules through compliance reviews and by levying fines.

Did you know?

- √ If your business provides services to a health care provider, in all likelihood, you are covered under HIPAA.
- √ The covered entity is required to take reasonable steps to mitigate a breach and report to HHS
- √ A sample Business Associate contract can be found at:

https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

- √ This resource was developed from the Department of Health and Human Services website

FACT 1: Covered Entities

Covered entities are defined as 1) health care providers (doctors, clinics, psychologists, dentists, chiropractors, nursing homes and pharmacies if they transmit information electronically for which HHS has a standard), 2) health plans (health insurance companies, HMOs, company health plans and government programs, such as Medicare, Medicaid, and the VA) or 3) health care clearinghouses (entities that process nonstandard health information received from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Many small businesses are covered entities under the act and must comply.

FACT 2: Business Associates

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.

HIPAA continued....

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. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information (PHI).

Business associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business associate services are: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. See the definition of "business associate" at 45 CFR 160.103.

So if you are a business that supports a covered entity it is imperative you understand your responsibilities under HIPAA to protect PHI.

FACT 3: Business Associate Contracts

Business Associate Contracts. A covered entity's contract or other written arrangement with its business associate must contain the elements specified in 45 CFR 164.504(e). For example, the contract must:

- Define the permitted and required uses of protected health information by the business associate;
- Ensure the business associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
- Require the business associate to use appropriate safeguards to prevent the use or disclosure of the PHI other than as provided for by the contract.

When a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is **required** to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). See HHS website for more information: https://www.hhs.gov/hipaa/for-professionals/index.html

Still have questions, need help?
Contact us at our "**Ask-an-Expert**" service,
web@thencss.org or visit us at the link below.