Cyber Liability

Complying with HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) addresses the privacy of individuals' health information by establishing a federal standard concerning the privacy of health information and how it can be used and disclosed.

Background

As health care institutions began storing larger volumes of private health data digitally, the need to protect this sensitive data from loss or theft grew. To address this risk, the U.S. Department of Health and Human Services (HHS) issued HIPAA's Privacy Rule and Security Rule in August 1996.

The Privacy Rule standards address the use and disclosure of individuals' health information (called "protected health information") by organizations subject to the Privacy Rule (called "covered entities") as well as standards for individuals' privacy rights to understand and control how their health information is used.

The Security Rule establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form. All covered entities were required to be in compliance by April 14, 2003, for the Privacy Rule and April 20, 2005, for the Security Rule.

What is a Covered Entity?

HIPAA defines "covered entities" as:

- Health care providers
- Health plans
- Health care clearing houses

If you are not sure whether your organization is a covered entity, the Centers for Medicare & Medicaid Services (CMS) has more information at their website.

HIPAA Requirements for Your Organization

Essentially, HIPAA has two primary components that your firm must follow:

- Administrative simplification, which calls for use of the same computer language industry-wide
- Privacy protection, which requires covered entities to take "reasonable" measures to protect patient health information

If your organization is a covered entity, you must comply with the following:

- Implement a required level of security for health information, including limiting disclosures of information to the minimum

necessary to accomplish the intended purpose. This standard does not apply to:
    - Disclosures to or requests by a health care provider for treatment purposes
    - Disclosures to the individual who is the subject of the information
    - Uses or disclosures made pursuant to an individual's authorization
    - Uses or disclosures required for compliance with HIPAA's Administrative Simplification Rules.
    - Disclosures to HHS when disclosure of information is required under the Privacy Rule for enforcement purposes.
    - Uses or disclosures that are required by other law.
- Designate a privacy officer and contact person
- Train employees on privacy policies
- Establish sanctions for employees who violate privacy policies
- Establish administrative systems that can respond to complaints about health information, respond to requests for corrections of health information by a patient, accept requests not to disclose for certain purposes and track disclosures of health information
- Create a privacy notice to patients concerning the use and disclosure of their protected health information

Cyber Liability and HIPAA

Patients' health information is extremely sensitive and should always be handled with the utmost care. All it takes is a simple misclick or misspelling to send private information to the wrong person. Such a mistake could lead to a lawsuit and/or fines

It's important to remember that HIPAA protects patients, not covered entities. That's why it's critical that your organization has a cyber liability insurance policy to cover any potential data breaches.

According to the Ponemon Institute's Cost of a Data Breach Survey, losses incurred from a data breach can add up, resulting in organizational costs that can quickly escalate to millions of dollars.

If a Data Breach Occurs

If a data breach occurs, notify your state's public health department immediately. Failing to do so can result in fines upward of $250,000. Under HIPAA, covered entities must immediately notify affected individuals following the discovery of a breach of unsecured protected health information.

Covered entities that experience a breach affecting more than 500 residents of a state or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the state or jurisdiction. In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information.

Plan Ahead

You can never see a data breach coming, but you can always plan for a potential breach. Contact Schauer Group today. We have the expertise to ensure you have the proper coverage to protect your company against a cyber attack.