HIPAA (Health Insurance Portability and Accountability Act) drives the Standards for Privacy of Individual Health Information (“Privacy Rule”) which establishes a set of national standards for the protection of certain health info. The privacy rule standards address the security, use, and disclosure of individual’s health info “PHI” (personal health info) by organizations subject to the privacy rules. HIPAA also governs the requirement to allow employees to transfer from one medical plan to another, without being subject to pre-existing conditions if they had creditable coverage. This article focuses on the privacy part of HIPAA.

Who is Covered by the Privacy Rule?
The rule applies to health plans, health care clearinghouses, business associates, and health care providers who handle individually identifiable health info and conduct certain financial or administrative transactions electronically. Even if your business is not covered by the privacy rule, you may elect to voluntarily put in place a privacy policy. The level to which the HIPAA Privacy Rule impacts a business is directly driven by the amount, frequency, and need to obtain PHI data. The greater these elements are the greater the risk, the greater the need to implement a clear, concise, secure and enforced privacy policy.

Employers are covered by the Privacy Rule, when they self-insure or enter into an insurance agreement with a provider. But they receive, manage, or disclose protected health info as a group health plan or perform certain record-keeping functions, like transmitting individual health records to a group plan. There may be other times where employers have access to confidential employee health data such as receiving PHI information from the employee’s doctors or directly from the employee.

What Information is Protected?
The following are examples of protected PHI “Personal Health Information”:

- health information including demographic info collected from an individual, in all forms including but not limited to electronic, written and/or oral;
- info created or received by a provider, health plan, employer, or health care clearinghouse;
- info relating to the physical or mental health or condition of an individual, at any time including past and future;
- info related to payment of health benefits;
- info identifying an individual or can be used to indentify an individual; and
- info in the possession or control of a covered entity (45 CFR §§ 106.103 & 164.501).

Use & Disclosure
Covered entity may not use or disclose PHI, except as permitted or required by the Privacy Rule section 164.524 (access) or 164.528 (accounting), to HHS for investigation or compliance application, health plan contact with enrollees, and provider contact with patient.

Authorization is required for uses and disclosures not otherwise permitted or required by the Rule. Covered entities must make reasonable efforts to limit the use or disclosure of, and requests for, PHI to minimum amount necessary to accomplish intended purpose.

Notice & Other Individual Rights
The Privacy Rule provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health info about the individual, as well as his or her rights and the covered entity’s obligations with respect to that info. Most covered entities must develop and provide individuals with this notice of their privacy practices.

Content of the Notice: Covered entities are required to provide a notice in plain language that describes how PHI may be used and disclosed, an individual’s rights and process, covered entities legal duties around PHI, and a single point of contact for explanation of privacy policy and practices. Other notice requirements and specifics can be found in 45 CFR 164.520(b).

Providing the Notice: A covered entity must make its notice available to any person, who asks for it, and must prominently post, and make available its notice on any web site it maintains that provides info about its customer services or benefits. A covered entity may email the notice to an individual if the individual agrees to receive an electronic notice. See 45 CFR 164.520(c) for the specific requirements for providing the notice.

Administrative Requirements
What is appropriate for one covered entity versus another will depend on the nature of the covered entity’s business, size, and resources. Each covered entity must analyze their own
needs, compare those to the administrative requirements indicate here, and implement a solution appropriate for their own environment.

- **Privacy Policies & Procedures**: develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.
- **Privacy Personnel**: designate a privacy official responsible for developing and implementing privacy policies and procedures and a contact person or contact office responsible for receiving complaints and providing individuals with info on privacy practices.
- **Workforce Training & Management**: train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions, have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures or the Privacy Rule.
- **Mitigation**: mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health info by its workforce or its business associates in violation of privacy policies and procedures or Privacy Rule.
- **Data Safeguards**: maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health info in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. For example, such safeguards might include shredding documents containing protected health info before discarding them, securing medical records with lock and key or pass code, and limiting access to keys or pass codes. Secure or encrypt all data stored or transferred electronically. Lock up PHI info and employee files. It is a good idea to separate PHI employee information from other employee file contents into a confidential, non-supervisor accessible file.
- **Complaints**: have procedures for individuals to complain about its compliance with privacy policies and procedures and the Privacy Rule, explain those procedures in its privacy practices notice, identify to whom individuals can submit complaints to at the covered entity and advise that complaints also can be submitted to the Secretary of HHS.
- **Retaliation & Waiver**: may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice the person believes in good faith violates the Privacy Rule, nor require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.
- **Documentation & Record Retention**: maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented.
- **Fully-Insured Group Health Plan Exception**: The only administrative obligations with which a fully-insured group health plan, that has no more than enrollment data and summary health info, is required to comply are (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents, if such documents are amended to provide for the disclosure of protected health info to the plan sponsor by a health insurance issuer or HMO that services the group health plan.

**Security Standards**

The HIPAA Security Standard consists of five major sections, administrative safeguards, physical safeguards, technical safeguards, organizational requirements and policy and document requirements. A good HIPAA policy will address, develop, and put in place steps dealing with each of these areas of risk.

**Notification of Breach**

The HITECH Act now imposes data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI." Under the HITECH Act "unsecured PHI" essentially means "unencrypted PHI."

In general, the Act requires patients be notified of any unsecured breach. If a breach impacts 500 patients or more then HHS must also be notified. Furthermore, notification is triggered whether the unsecured breach occurred externally or internally.

**State Law**

In general, State Laws contrary to the Privacy Rule are preempted by the federal requirement, which means the federal requirement will apply.

Compliance with the HIPAA Privacy Rule is not optional, it is the law. Employers will avoid costly fines by following the requirements described in this article.

By Deborah Siddoway, HR Coach, HR Service, Inc., (801) 685-8400.

**References sited:**

**HIPAA Compliance Assistance**

For assistance in HIPAA compliance or any HR support need, contact HR Service, Inc. at: (801) 685-8400 or Ken@hrserviceinc.com.
Visit us on-line at: www.HRServiceInc.com