

# HIPAA

## **About HIPAA - Health Insurance Portability and Accountability Act**

The Health Insurance Portability and Accountability Act (HIPAA) was initially created to protect health insurance coverage for employees who changed or lost their jobs (portability). The Administrative Simplification portion was created in order to increase the effectiveness and efficiency of health care and for the protection of health information (accountability). The "portability" portion of HIPAA has been in effect since 1996, but we are just now beginning to see the "accountability" portion come into play.

HIPAA is the most comprehensive health care privacy legislation ever passed in the United States. All health care providers (hospitals, physicians, pharmacies, dentists, etc.), health plans, and health care clearinghouses (3rd party vendors for billing, claims, etc) must comply. HIPAA covers information in electronic, written, and oral forms. In order to accomplish the goals set forth by HIPAA, the Department of Health and Human Services (DHHS) created three sets of standards:

- Electronic Transactions and Code Sets
- Privacy
- Security

## **Electronic Transactions Standards**

In the past, health providers and plans have used many different electronic formats to transact medical claims and related business. Implementing a national standard is intended to result in the use of one format, thereby "simplifying" and improving the efficiency of transactions nationwide. Specifically targeted are eight administrative and financial transactions:

- claims encounter and coordination of benefits (837)
- remittance advice (835)
- eligibility inquiry and response (270/271)
- status inquiry and response (276/277)
- authorization request and response (278)
- enrollment and disenrollment (834)
- premium payments (820)

Healthcare providers must use these standards if they submit transactions electronically to a health plan. However, Medicare requires electronic transactions, and all Medicare providers must adopt the standards for these transactions.

The rule also defines a series of code sets to support these transactions. These include ICD-9-CM for diagnoses and inpatient services, HCFA Common Procedural Coding System (HCPCS) for healthcare procedures, equipment, and supplies, and National Drug Code (NDC) for drugs. Fortunately, the code sets proposed as HIPAA standards are already used by most providers and health plans.

## **Unique Identifier Standards**

In the past, healthcare organizations have used multiple identification formats when conducting business with each other - a confusing, error-prone, and costly approach. It is expected that standard identifiers will reduce these problems.

The Unique Employer Identifier Standard, published in 2002, adopts an employer's tax ID number or employer identification number (EIN) as the standard for electronic transactions. The compliance date for this standard is July 30, 2004.

The Unique Healthcare Provider Identifier Standard was published January 23, 2004. This final rule establishes a standard national provider identifier (NPI) for all healthcare providers under HIPAA. Healthcare providers may apply for NPIs beginning on, but no earlier than, May 23, 2005. The compliance date for this standard is May 23, 2008.

The Unique Health Plan (Payer) Identifier is in a proposed status. This rule would implement a standard identifier to identify health plans that process and pay certain electronic healthcare transactions. The estimated publication date for this is not known.

### **Claim Attachment Standards**

This rule proposes an electronic standard for claim attachments required by HIPAA. It would be used to transmit clinical data, in addition to the data contained in the claim standard, to help establish medical necessity for coverage. The estimated publication date is August 2004.

### **Privacy Standards**

HIPAA's Privacy Standards for the first time create national standards to protect individual's medical records and other personal health information. Patients will have more control over their health information. The rule sets boundaries on the use and release of health records, establishes appropriate safeguards that health care providers must achieve to protect the privacy of health information, holds violators accountable, with civil and criminal penalties, and enables patients to find out how their information may be used and what disclosures of their information have been made. It also gives patients the right to examine and obtain a copy of their own health records and request corrections. Compliance with HIPAA Privacy Standards began April 14, 2003.

### **Modifications to Standards for Privacy of Individually Identifiable Health Information**

Modifications to Standards for Privacy of Individually Identifiable Health Information were published 08/14/02. The compliance date remained 04/14/2003. The modification changed the standards for:

- Marketing
- Consent and Notice
- Uses and Disclosures Regarding FDA
- Regulated Products and Activities
- Incidental Use and Disclosure
- Authorization
- Minimum Necessary
- Parents and Minors
- Business Associates
- Research
- Limited Data Set
- Hybrid Entities
- Health Care Operations: Changes in Legal Ownership
- Group Health Plan Disclosures of Enrollment and Disenrollment Information
- Accounting of Disclosures
- Disclosure for Treatment, Payment, or Health Care Operations of Another Entity
- Protected Health Information: Exclusion for Employment

### **Security Standards**

The Final Security Rule was published on February 20, 2003 with a compliance date of April 21, 2005. This rule is the first of its kind in healthcare-namely that all covered organizations must comply with the provisions specified by the Federal Government. In general terms, this rule requires that covered entities must do certain things:

- Ensure the confidentiality, integrity and availability of all electronic protected health information (PHI) the covered entity creates, receives, maintains or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the rule; and
- Ensure compliance by the workforce of the covered entity.

The specific areas that have to be addressed are broken down into three general areas: physical safeguards, technical safeguards and administrative safeguards. These safeguards are further

broken down into 18 security standards with 42 specific security areas that must be addressed by the covered organization.

This rule represents what would be considered the best practices by other industries but is specifically tailored to healthcare. Some of the requirements in the rule are already being done to a degree. For example, the rule requires security training for employees and the use of authentication mechanisms to access computers. It also requires the creation and enforcement of policies and procedures to govern the way we work. Other requirements such as the need for encrypting electronic transmissions that contain PHI and that travel outside of our network are new and will have to be addressed in order to achieve compliance. Finally, the Security Rule does not tell us what technology to use nor how to go about creating some of the policies that we will need. It does require that we determine what approach to take that will best suit our needs while still meeting the basic obligations in each area.

### **Frequently Asked Questions**

**What is HIPAA?**

HIPAA, the Health Insurance Portability and Accountability Act is the most comprehensive healthcare privacy legislation ever passed in the United States. All health care providers (hospitals, physicians, pharmacies, dentists, etc.), health plans and health care clearinghouses (3rd party vendors for billing, claims, etc.), must comply. HIPAA protects medical records and other individually identifiable health information whether it is on paper, in computers or communicated orally. Orlando Health must comply with HIPAA.

**What is PHI?**

PHI stands for protected health information. It is data, including demographic information, collected from an individual and created or received by South Lake Hospital that: (1) relates to the past, present or future physical or mental condition of an individual, the provision of healthcare to an individual, or the past, present, or future payment for the provision of healthcare to an individual. Secondly, it can be used as an identifier to identify an individual.

**What does the Privacy Rule require the average healthcare provider, including South Lake Hospital, to do?**

Here are some of the requirements:

- Provide information to patients about his or her privacy rights as well, as how information can be used.
- Obtain authorization from patients for certain uses and disclosures of PHI.
- Adopt clear privacy procedures.
- Train employees so that they understand the privacy procedures.
- Designate an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Secure patient records containing PHI so that they are not readily available to those who do not need them.

**May physicians and other healthcare providers share patient health information for treatment purposes without the patient's authorization?**

Yes. The Privacy Rule allows doctors, nurses, hospitals, lab technicians and healthcare facilities to use or disclose PHI for treatment purposes without the patient's authorization. Other uses and disclosures may require an authorization in compliance with state law. Consult Health Information Management for specific guidelines.

**What is the Notice of Privacy Practices?**

The Notice of Privacy Practices is a document provided to all patients one time upon their registration for care at South Lake Hospital. The notice describes how patient healthcare information may be used and disclosed and how the patient or the patient's legal representative may obtain access to their health information.