

The Parts of HIPAA

There are 3 main areas that comprise HIPAA and have compliance deadlines. HIPAA not only carries the following deadlines, but also defined monetary and imprisonment penalties for organizations that fail to comply with the new federal law.

Deadlines:

- | | |
|------------------------------|----------|
| • Privacy | 04/14/03 |
| • Transactions and Code Sets | 10/16/03 |
| • Security | 04/21/05 |

Purpose of Privacy

- Limit the release of protected information without consent
- Inform consumers about how their health information is being used
- Give patient access to their own health records and the right to request amendments or make corrections
- Restrict the amount of information used and disclosed to the "Minimum Necessary"
- Create new criminal and civil penalties for improper use and disclosure of information
- To protect the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information
- To restore trust in the health care system among consumers, health care professionals, and the multitude of organizations and individuals committed to the delivery of care
- To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection that builds on efforts by states, health systems, individual organizations and individuals

Why Worry About Privacy?

- Patients are concerned because improper use of their medical information may cause:
 - Embarrassment
 - Financial disadvantage
 - Unwillingness to share all necessary information with health care professionals
 - Loss of confidence in care providers
- Criminal Penalties
 - Executives can end up in jail. Criminal penalties are established for knowingly disclosing individually identifiable health information inappropriately
 - Penalties are up to \$250,000 fine and/or 10 years imprisonment
- Potential Penalties of Non-Compliance
 - JCAHO, CMS, OIG & OCR will cite non-compliance
 - Risk to reputation – not protecting patient data
 - Lost opportunities and Negative Business impacts
 - Lack of awareness by providers and medical groups
 - Magnitude of change will increase consumer and provider disruption

HIPAA Objectives

- Understand the importance of Privacy in Healthcare
- Understand the major components of the Privacy Rule
- Understand Patients' Rights under HIPAA
- Understand how HIPAA impacts daily work
- Understand Notice of Privacy Practices and be able to communicate it to others
- Understand the idea of "minimum necessary" as it relates to use and sharing of Protected Health Information (PHI)
- Define Protected Health Information
- Understand all of the consequences for privacy breaches

What is HIPAA?

Congress enacted the Health Insurance Portability and Accountability Act of 1996, otherwise known as HIPAA. The HIPAA Privacy Rule – finalized on August 14, 2002 – ensures that personal medical information you share with doctors, hospitals, and others who provide and pay for healthcare is protected. Numerous states and the federal government enacted protections for health care information.

HIPAA was originally intended to support:

- The portability of health insurance
- Improved fraud and abuse protections

More rules were added to improve administration efficiencies, reduce paperwork and ensure confidentiality and privacy to medical information.

The goal of HIPAA Privacy

- The goal of the regulation is to protect personal health records. The U.S. Department of Health and Human Services and the Office of Civil Rights regulates HIPAA.

Definitions

Privacy – the individual's right to keep certain information to him or herself, with the understanding that the information will only be used or disclosed with his or her permission.

Protected Health Information (PHI) – Any information (spoken, stored, emailed, typed, printed, etc.) created or received by you that relates to:

- the medical condition of an individual
- the care received by an individual
- and/or the payment for an individual's care

Covered entities could use and disclose protected health information without authorization for treatment, payment and health care operations; but all other disclosures require an individual's authorization.

Covered Entity – Health plans, health care clearinghouses, health care providers, self-insured employers, home health care providers, physician practitioners and special diagnostic centers that conduct certain types of transactions in electronic form.

Use – Sharing PHI

Disclosure – Sharing PHI with people outside

Definitions (continued)

TOP = Treatment, Payment and Operations

- HIPAA makes a significant distinction with how you can use and disclose information
- Releasing information for TPO does not require an authorization
- Releasing information for reasons other than TPO requires a signed authorization from a patient
- TOP includes:
 - All treatment purposes
 - All interactions with insurance and other companies to get bills paid
 - Operations are things such as: quality assessment activities, employee review activities, training of medical students, and conducting or arranging for other business activities.

Minimum Necessary

- Must limit the PHI is uses, discloses, or requests to the minimum necessary to achieve the given purposes
 - Non-routine uses, disclosures and requests must be reviewed on a case-by-case basis
- Does not apply to:
 - Treatment disclosures or requests
 - Use or disclosure made with an authorization
 - Disclosures to/uses by the individual
 - Disclosures to DHHS for compliance; other uses and disclosures for compliance
 - Uses or disclosures as required by law
- Application of Minimum Necessary
 - Use as little PHI as possible to do your job
 - Look at as little as possible to do your job
 - Disclose the minimum necessary to others outside
 - Example: Insurance companies do not always need complete medical records.

18 Unique Identifiers

- Names
- Geographic subdivisions smaller than a State, including: street address, city, county, precinct, zip code
- Dates (except year) directly related to an individual (e.g., DOB, discharge date, date of death, and all ages over 89)
- Telephone numbers
- Fax numbers
- Electronic mail addresses

- Social Security Numbers
- Medical Record Numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic or code

Patient Rights - Overview

Individuals have the right to:

- Receive a Notice of Privacy Practices
- Access their PHI (with some restrictions)
- Request amendment of their PHI
- Receive a record of certain disclosures of their PHI made within previous 6 years
- Request restrictions on uses and disclosures
- Revoke their authorization
- Request receipt of communication of their PHI by alternative means/location

Notice of Privacy Practices

The Rule

- Must tell individuals how their protected health information is used and disclosed. Must do this by:
 - Providing a Privacy Notice and
 - Making a good faith effort to obtain written acknowledgement of receipt
- The Notice of Privacy Practices describes
 - Required uses and disclosures – to Secretary DHHS and to individual
 - Permitted uses and disclosures – with authorization/permission and without authorization/permission
- Beginning April 14, 2003, must obtain signed acknowledgement from every patient that he/she received the notice before sharing their information for treatment, payment and operations.

Use and Disclosure

- Authorization for Use & Disclosure is not needed for:
 - Treatment, payment, healthcare operations
 - Abuse, neglect, or domestic violence reporting
 - Judicial and administrative proceedings
 - Public Health activities
 - Health Oversight Agencies
 - Law Enforcement purposes
 - Coroners and medical examiners (if for purposes of identifying a person or cause of death)
 - Cadaveric Eye and Tissue Donation
 - Research pursuant to a waiver
- Authorization to Use and Disclose PHI must be obtained from a patient:
 - When the use and disclosure of PHI is for reasons other than TPO
 - Authorizations cannot be blanket authorizations. For example, a patient cannot say "release entire medical record whenever necessary."
 - Authorizations must be written in plain language, include a specific and meaningful description of what information will be used and disclosed, list who may use or disclose the information, list to whom the PHI will be disclosed, explain why the use or disclosure is being made (each purpose, and include an expiration date)
- Authorization Required – Required Elements, the authorization must include:
 - A notice that authorization may be revoked
 - A notice that the information may be disclosed to others not subject to the Privacy Rule
 - A notice that you may or may not condition treatment or payment on the individual's signature
 - The individual's signature and date
- Authorization to Use and Disclose PHI may be revoked – revocation must be in writing

Business Associates

- Business Associates must follow the Privacy Rule indirectly since they have contracts
- Business Associates are people or companies that perform a service on behalf of you involving the use or disclosure of individually identifiable health information such as:
 - claims processing or administration; data analysis, processing or administration; utilization review; quality assurance and practice management
 - also includes legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services

- HIPAA Compliant Contracts Must include:
 - Restrictions on how PHI may be used or disclosed
 - A promise to protect the PHI
 - A promise to return PHI at end of contract
 - Assurance to make PHI available for compliance purposes and audits

Conclusion

- The Privacy regulation is about individual rights
- You cannot access, use or disclose PHI (beyond TPO) without proper consent or authorization from a patient unless an exception can be identified
- Confidential subjects are not discussed openly and should be only discussed in a reasonably private setting
- The Privacy rules cover PHI in all media: electronic, paper, or oral
- Financial and criminal penalties can result from willful misuse or inappropriate disclosure of PHI
- Criminal penalties are:
 - up to \$50,000 and one year in prison for obtaining or disclosing PHI
 - up to \$100,000 and up to 5 years in prison for obtaining PHI under "false pretenses"
 - up to \$250,000 and up to 10 years in prison for obtaining or disclosing PHI with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

Lake Anna Chiropractic Inc.

HIPAA TRAINING ACKNOWLEDGEMENT FORM

I have received and read the HIPAA informational packet as provided
by *Lake Anna Chiropractic Inc.*

Employee Signature

Date

Please print name