

HIPAA OVERVIEW

**Salida Fire
Protection
District**

What is HIPAA?

**Health Insurance
Portability and Accountability Act.**

PURPOSE – TITLE II ADMINISTRATIVE SIMPLIFICATION

- To increase the efficiency and effectiveness of the entire health care system through:
 - ✓ The electronic exchange of information
 - ✓ The standardization of that information
- To enhance the security and privacy of Protected Health Information (PHI) throughout the entire health system

PRIVACY RULE: WHAT DOES IT DO?

HIPAA regulates the use or disclosure of
Protected Health Information (PHI)

WHAT IS PHI?

Health and demographic information about an individual that is transmitted or maintained in any medium where the information:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future
 - ✓ Physical or mental health condition of an individual, or
 - ✓ Provision of health care to an individual, or
 - ✓ Payment for the provision of health care to an individual

INDIVIDUAL IDENTIFIERS

- | | |
|--|---|
| 1. Name | 6. E-Mail Address |
| 2. Geographic subdivisions smaller than a State <ul style="list-style-type: none">– Street Address– City– County– Precinct– <i>Zip Code & their equivalent geocodes, except for the initial three digits</i> | 7. Social security numbers |
| 3. <i>Dates, except year</i> <ul style="list-style-type: none">– <i>Birth date</i>– <i>Admission date</i>– <i>Discharge date</i>– <i>Date of death</i> | 8. Medical record numbers |
| 4. Telephone numbers | 9. Health plan beneficiary numbers |
| 5. Fax number | 10. Account numbers |
| | 11. Certificate/license numbers |
| | 12. Vehicle identifiers and serial numbers, including license plate numbers |
| | 13. Device identifiers and serial numbers |
| | 14. Web universal resource locations (URLs) |
| | 15. Internet Protocol (IP) address numbers |
| | 16. Biometric identifiers, including finger and voice prints |
| | 17. Full face photographic images and any comparable images |
| | 18. Any other unique identifying number, characteristic, or code |

PERMITTED USES & DISCLOSURES

HIPAA *permits* the use or disclosure *only* for the following purposes:

- Treatment
- Payment
- Health Care Operations

(These are referred to as “TPO”)

MANDATED USES & DISCLOSURES

- HIPAA *mandates* the disclosure of PHI for certain purposes such as:
 - ✓ Health oversight activities
 - ✓ Judicial and administrative proceedings
 - ✓ Law enforcement purposes
 - ✓ Organ donation
- All other uses or disclosures require an authorization

HEALTH CARE OPERATIONS

Any of the following activities of a Covered Entity:

- Quality assessment and improvement and population-based activities
- Peer review and credentialing activities
- Underwriting, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance
- Medical review, legal services, and auditing
- Business planning and development
- Business management and general administrative activities

AUTHORIZATION

- Authorization must be obtained for ALL uses and disclosures other than TPO or those mandated under law
- Authorizations must include:
 - ✓ A description of the information to be disclosed
 - ✓ The name of the person or entities to whom the information will be disclosed
 - ✓ An expiration date
 - ✓ Information regarding right to revoke
 - ✓ Date and signature

PRIVACY NOTICE

Privacy Notices Must:

- Be in plain language
- Contain a description and example of TPO
- Contain a description and example of other uses and disclosures not requiring Authorization
- Include statements about an individual's rights
- Include statements about the Covered Entity's duties
- Describe the complaint process
- Provide other specific requirements

MINIMUM NECESSARY

A requirement that only “minimum necessary disclosures” may be made to accomplish the intended purpose of the *use, disclosure, or request* for PHI.

MINIMUM NECESSARY

- Internal Requirements:
 - ✓ Identify workforce who need to access PHI
 - ✓ For each class, category or person identified, limit access based on need-to-know
- External Requirements:
 - ✓ Limit access to what is needed to accomplish the purpose for which the request was made
 - ✓ Each request that is non-routine should be reviewed to determine whether it is reasonably necessary

RESEARCH

To use or disclose PHI for research purposes, Covered Entities must obtain either:

- Written authorization from the research subject.
- Permission from the Institutional Review Board (IRB) or Privacy Board to waive the authorization.

IRB WAIVER OF AUTHORIZATION

The following criteria must be met before the IRB can waive the patient authorization requirement for research:

- ✓ Use of PHI will pose minimal risks to the subject's welfare and privacy rights.
- ✓ Research can not practically be conducted without the waiver or access to PHI.
- ✓ Covered entity must protect PHI from inappropriate use or disclosure.
- ✓ Researcher must provide written assurances that PHI will not be reused or disclosed, except as required by law.

INDIVIDUAL RIGHTS

Individuals have the right to:

- Receive written notice of privacy practices
- Request restrictions on uses & disclosures
- Access, inspect & copy their PHI
- Request amendment or correction of their PHI
- Receive an accounting of disclosures of their PHI (except those related to treatment, payment, & operations)

ADMINISTRATIVE REQUIREMENTS

- Designate a privacy officer with primary responsibility for ensuring compliance with the regulations
- Establish training programs for all members of the workforce
- Implement appropriate policies & procedures to prevent intentional and accidental disclosures of PHI

ADMINISTRATIVE REQUIREMENTS

- Establish a system for receiving and responding to complaints regarding the Covered Entity's privacy practices
- Implement appropriate sanctions for violations of the privacy guidelines
- Make reasonable efforts to limit information to minimum necessary to accomplish a person's purpose/job

ENFORCEMENT

- **The Public.** The public will be educated about their privacy rights and will not tolerate violations to their privacy! Expect Class Action lawsuits.
- **Office For Civil Rights (OCR).** Designated the enforcement agency concerning privacy regulations. They will provide guidance and monitor compliance.
- **Department of Justice (DOJ).** Involved in criminal privacy violations. Expect fines and penalties to be high.

PENALTIES - FAILURE TO COMPLY

- Civil
 - ✓ \$100 per violation per person up to a maximum of \$25,000 per person per year per standard violated
- Criminal
 - ✓ Up to \$50,000, 1 year in prison, or both, for inappropriate use of PHI
 - ✓ Up to \$100,000, 5 years in prison, or both for using PHI under false pretenses
 - ✓ Up to \$250,000, 10 years in prison or both, for the intent to sell or use PHI for commercial advantage, personal gain, or malicious harm

RESOURCES

<http://www.cms.hhs.gov/hipaa/hipaa2> – For frequently asked questions, links to other HIPAA sites, and information on the law, regulations, and enforcement

<http://www.hhs.gov/ocr/hipaa/> - U.S. Department of Health and Human Services' Office for Civil Rights frequently asked questions

<http://www.hhs.gov/ocr/moneypenalties.html> – Interim final rule: Civil Money Penalties