

## Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act is the most sweeping legislation to affect the health care system in over 30 years. Congress perceived there to be increased concern about privacy of medical information and increased use of interconnected electronic information systems in health care.

This legislation has four key goals:

- Improve consumer control of their health information
- Change the way health care is provided and information is managed
- Health care industry to speak the same language
  - Provide seamless exchange of clinical information between health care providers by 2005
- Save the industry administrative \$\$\$!
  - This will be accomplished by reducing the cost of administrative overhead in health care by 50% by 2003

### COMPLIANCE SCHEDULE

#### Transactions & Code Sets – Compliance date October 16, 2003

- Uniform National Standards for electronic transmission of certain transactions
- Single Identification Numbers for providers, employers, health plans and patients

#### Security Standards – Compliance date to be announced

- Ensure security of electronic health information and electronic signatures

#### Privacy Standards – Compliance date April 14, 2003

### COVERED ENTITIES

As required by HIPAA, the final regulation covers health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., electronic billing and funds transfers) electronically.

### INFORMATION PROTECTED

All medical records and other individually identifiable health information used or disclosed by a covered entity in any form, whether electronically, on paper, or orally, are covered by the final rule.

### CONSUMER CONTROL OVER HEALTH INFORMATION

Under the final rule, patients will have significant new rights to understand and control how their health information is used.

Patient education on privacy protections. Providers (TVHD) and health plans will be required to give patients a clear written explanation of how the covered entity may use and disclose their health information. This is called a “Privacy Notice”.

Ensuring patient access to their medical records. In California patients have been able to obtain a copy of their medical records for many years. However, this new legislation makes this an option for patients in all states to see and get copies of their records, and request amendments. In addition, a history of non-routine disclosures must be made accessible to patients. A separate patient authorization must be obtained for non-routine disclosures and most non-health care purposes. Patients will have the right to request restrictions on the uses and disclosures of their information.

Providing recourse if privacy protections are violated. People will have the right to file a formal complaint with a covered provider or health plan, or with HHS, about violations of the provisions of this rule or the policies and procedures of the covered entity.

#### BOUNDARIES ON MEDICAL RECORD USE AND RELEASE

With few exceptions, such as appropriate law enforcement needs, an individual's health information may only be used for health purposes. Ensuring that health information is not used for non-health purposes. Health information covered by the rule generally may not be used for purposes not related to health care - such as disclosures to employers to make personnel decisions, or to financial institutions - without explicit authorization from the individual.

Providing the minimum amount of information necessary. In general, disclosures of information will be limited to the minimum necessary for the purpose of the disclosure. However, this provision does not apply to the disclosure of medical records for treatment purposes because physicians, specialists, and other providers need access to the full record to provide quality care.

#### ENSURE THE SECURITY OF PERSONAL HEALTH INFORMATION

The final rule establishes the privacy safeguard standards that covered entities must meet, but it gives covered entities the flexibility to design their own policies and procedures to meet those standards. The requirements are flexible and scalable to account for the nature of each entity's business, and its size and resources.

Covered entities (including TVHD) generally will have to:

Adopt written privacy procedures. These include who has access to protected information, how it will be used within the entity, and when the information may be disclosed. Covered entities will also need to take steps to ensure that their business associates protect the privacy of health information.

Train employees and designate a HIPAA (privacy) officer. The Tehachapi Valley Healthcare District HIPAA Office can be reached at (661) 822-3241, extension 343. Covered entities will need to train their employees in their privacy procedures, and must designate an individual to be responsible for ensuring the procedures are followed.

#### ESTABLISH ACCOUNTABILITY FOR MEDICAL RECORDS USE AND RELEASE

In HIPAA, Congress provided penalties for covered entities that misuse personal health information.

## PENALTIES

Civil penalties. Health plans, providers and clearinghouses that violate these standards will be subject to civil liability. Civil money penalties are \$100 per violation, up to \$25,000 per person, per year for each requirement or prohibition violated.

Federal criminal penalties. Under HIPAA, Congress also established criminal penalties for knowingly violating patient privacy. Criminal penalties are up to \$50,000 and one year in prison for obtaining or disclosing protected health information; up to \$100,000 and up to five years in prison for obtaining protected health information under "false pretenses"; and up to \$250,000 and up to 10 years in prison for obtaining or disclosing protected health information with the intent to sell, transfer or use it for commercial advantage, personal gain or malicious harm.

## BALANCING PUBLIC RESPONSIBILITY WITH PRIVACY PROTECTIONS

In limited circumstances, the final rule permits - but does not require - covered entities to continue certain existing disclosures of health information without individual authorization for specific public responsibilities.

These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research, generally limited to when a waiver of authorization is independently approved by a privacy board or Institutional Review Board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security.

All of these disclosures could occur today under existing laws and regulations, although the privacy rule generally establishes new safeguards and limits. If there is no other law requiring that information be disclosed, covered entities will use their professional judgments to decide whether to disclose any information, reflecting their own policies and ethical principles.

## SPECIAL PROTECTION FOR PSYCHOTHERAPY NOTES

Psychotherapy notes (used only by a psychotherapist) are held to a higher standard of protection because they are not part of the medical record and are never intended to be shared with anyone else. All other personal health information is considered to be sensitive and protected consistently under this rule.

## EQUIVALENT REQUIREMENTS FOR GOVERNMENT ENTITIES

The provisions of the final rule generally apply equally to private sector and public sector entities. For example, both private hospitals and government medical units have to comply with the full range of requirements, such as providing notice, access rights and requiring consent for routine uses.

## COST OF IMPLEMENTATION

The final rule projected the implementation costs at \$17.6 billion over 10 years - a figure more than offset by the \$29.9 billion in projected savings under the final electronic transactions regulation issued in August 2000.

## PRESERVING EXISTING, STRONG STATE CONFIDENTIALITY LAWS

As required by the HIPAA law itself, stronger state laws (like those covering mental health, HIV infection, and AIDS information) continue to apply. These confidentiality protections are cumulative; the final rule will set a national "floor" of privacy standards that protect all Americans, but in some states individuals enjoy additional protection. In circumstances where states have decided through law to require certain disclosures of health information, the final rule does not preempt these mandates.

## COMPLIANCE AND ENFORCEMENT

The rule will be enforced by the HHS Office for Civil Rights (OCR). Guidance and other information about the new regulation are available on the Web at [www.hhs.gov/ocr/hipaa](http://www.hhs.gov/ocr/hipaa)

Rev. 09/27/03/cms