

## CHAPTER 33

### HIPAA PRIVACY REGULATIONS

#### I. INTRODUCTION

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress and signed into law by President Clinton in 1996. Most people are familiar with the portability provisions, those provisions which allow you to maintain health insurance benefits when changing jobs. However, many people are unfamiliar with the administrative simplification provisions. These provisions included requirements for the electronic transmission of health care information, including electronic signatures, unique identifiers, standards for designated transactions and security and privacy standards for health information.

The Department of Health and Human Services issued the final regulations on December 28, 2000. The final regulations greatly expanded the scope of the privacy rule under the proposed regulations. Most covered entities needed to be in compliance with the privacy rule by April 14, 2003.

#### II. THE BASICS OF THE FINAL HIPAA PRIVACY REGULATIONS

The basic philosophy of the HIPAA privacy regulations is that the use and exchange of health information should be relatively easy for health care purposes and relatively difficult for other purposes. The basic purpose of the regulations is to ensure the privacy of health information that is maintained or transmitted by health care providers, health plans, and health care clearinghouses. The basic rule is as follows:

Covered entities may not use or disclose individually identifiable health information unless authorized by the individual or permitted under the regulations.

The HIPAA privacy regulations do not apply to every person or entity nor do the regulations apply to every piece of information. Consequently, you must answer the following questions to determine whether the regulations apply:

1. Are you a covered entity?
2. Is the health information protected?

If you answer yes to both of the foregoing questions than the HIPAA privacy regulations apply to that piece of information.

### **III. KEY DEFINITIONS UNDER HIPAA PRIVACY REGULATIONS**

#### **A. COVERED ENTITY**

There are three types of covered entities that are subject to the HIPAA regulations. The three covered entities are health care plans; health care clearinghouses; and health care providers who transmit any health information in electronic form in connection with a transaction covered by HIPAA.

A health care provider is any person or organization that furnishes, bills, or is paid for, health care in the normal course of business and transmits health information in electronic form in connection with HIPAA transactions (claims, coordination of benefits, referral certification and authorization, injury reporting, etc.) is subject to the HIPAA privacy regulations. Examples include:

1. Hospitals, SNF's and CORF's;
2. Home health agencies and Hospice programs;
3. Providers of physicians' services;
4. Providers of diagnostic services;
5. Providers of outpatient therapy services;
6. Physician assistants and nurses in limited circumstances;
7. Providers of X-ray, radium, and radioactive isotope therapy, including materials and services of technicians; and
8. Providers of durable medical equipment and prosthetic devices (other than dental).

#### **B. PROTECTED HEALTH INFORMATION (PHI)**

Protected Health Information (PHI) is individually identifiable health information that is transmitted or maintained by electronic media or in any other form or medium. To further break down this definition of PHI, individually identifiable health information includes, information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

3. That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Some examples of individually identifiable health information are:

1. Name or relatives' names;
2. Address;
3. Employer;
4. Date of birth;
5. Telephone and telefax numbers;
6. E-mail and IP address;
7. Social Security Number/Medical Record Number;
8. Member or account number;
9. Driver's license number; and
10. Voice, fingerprints, or photos.

Electronic media is the source or target of the information exchanged. Examples of electronic media are floppy disks, the internet, dial-up lines, leased lines and private networks. Other forms or medium expands the definition of PHI to include paper records and, arguably, oral health information.

#### **IV. GENERAL RULES FOR THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION UNDER HIPAA REGULATIONS**

Once you determine that you and the information you wish to use or disclose is covered by HIPAA, you must either obtain consent from the patient, provide the patient with an opportunity to object or obtain an authorization form to use or disclose any PHI prior to using or disclosing the PHI, unless one of twelve exceptions applies.

In addition to requiring covered entities to have the proper forms in place prior to using and disclosing PHI, the regulations also provide additional rules, which are applicable to any use or disclosure of PHI made pursuant to the regulations. First, the regulations limit the amount of PHI that may be used, disclosed or requested by a covered entity to that which is the minimum necessary amount to accomplish the intended purpose of the use, disclosure, or request. There are notable exceptions to the rule. Second, prior to any disclosure a covered entity must verify the identity and authority of a person requesting PHI, if unknown to the covered entity, and obtain any required documentation, statements, or representations

from the person requesting the PHI.

**A. CONSENT FOR USE OR DISCLOSURE TO CARRY OUT TREATMENT, PAYMENT OR HEALTH CARE OPERATIONS**

When a covered health care provider desires to use or disclose PHI for treatment, payment or health care operations, the provider must obtain the individual's consent prior to using or disclosing PHI for those purposes. However, a consent form is not adequate for use or disclosure of psychotherapy notes, which requires an authorization form. A covered health care provider may condition treatment on the provision by the individual of a consent.

There are two notable exceptions to the rule: the covered health care provider has an indirect treatment relationship (i.e. pathologists or radiologists) with the individual; or the covered health care provider created or received the PHI in the course of providing healthcare to an inmate. In these cases, a consent form is not required for the provider to use or disclose PHI for treatment, payment or health care operations.

The consent may be obtained at a later time when an emergency treatment situation exists. An emergency situation is when the provider is required by law to treat the individual and is unable to obtain the consent, or when the provider is unable to obtain consent due to substantial communication barriers and the provider determines that consent to receive treatment is clearly inferred from the circumstances.

The regulations set forth the required content for consent forms. A consent form may be combined with other types of written legal permission from the individual, if the PHI consent is separate and separately signed and dated. However, a single document may not contain both a consent and the notice of privacy practices. Covered entities must document and retain any signed consent forms. Finally, consents may be revoked at any time, so long as the revocation is in writing.

**B. PROVIDING AN OPPORTUNITY FOR THE INDIVIDUAL TO AGREE OR TO OBJECT**

There are only two instances when a covered entity must provide an individual with an opportunity to agree or object prior to using or disclosing PHI. These two instances are when placing PHI into a facility directory and when making disclosures to persons involved in the individual's care, including disclosures for notification purposes.

**C. THE EXCEPTIONS TO THE PRIVACY REGULATIONS**

The requirements of the privacy rule do not apply to uses or disclosures that are required by law, disclosures made to the individual or pursuant to an authorization initiated by the individual, disclosures to or requests by a health care provider for treatment purposes, uses or disclosures that are required for compliance with the regulations implementing the other administrative simplification provisions of HIPAA, or disclosures to the Secretary of HHS for purposes of enforcing this rule.

**V. WHEN IS AN AUTHORIZATION REQUIRED**

Generally, a covered entity may not use or disclose PHI without a valid authorization, unless permitted by HIPAA. In other words, this is a catchall. Unlike the rules for consent forms, a covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization with limited exceptions. Use or disclosure of PHI must be consistent with the authorization.

A covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, with limited exceptions which include: treatment by the originator, training, legal actions by the patient or oversight agencies.

The regulations set forth requirements for the content of authorizations. Generally, an authorization will be much more extensive than a consent. Like consents, a covered entity must document and retain any signed authorization. Unlike a consent form, an authorization form must contain an expiration date and expires at that time or earlier if revoked by the individual prior to the expiration date. The authorization may be revoked by the individual at any time, so long as the revocation is in writing.

**VI. INDIVIDUAL RIGHTS**

The HIPAA privacy regulations establish rights for patients. These rights include the following:

1. Right to notice of the covered entity's privacy practices;
2. Right to access their own PHI;
3. Right to amend their own PHI;
4. Right to receive an accounting of the covered entity's disclosures of their PHI; and
5. Right to request privacy protection for their own PHI.

**VII. ADMINISTRATIVE REQUIREMENTS**

HIPAA also imposes administrative requirements on covered entities, including:

1. Designating a privacy official;
2. Designating a contact person or office for receiving complaints;
3. Training all members of the workforce on the required PHI policies and procedures, as necessary and appropriate for the members of the workforce to carry out their function within the covered entity;

4. Implementing appropriate administrative, technical, and physical safeguards to protect the privacy of PHI;
5. Implementing a complaint process and documenting all complaints received and the disposition of the complaints;
6. Implementing and applying appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures or HIPAA requirements, sanctions must be documented;
7. Mitigating, if possible, any known harmful effect of a use or disclosure of PHI that violates the covered entity's policies and procedures or HIPAA by the covered entity or its business associate;
8. Refraining from intimidating or retaliatory acts against individuals exercising their rights under HIPAA;
9. A covered entity may not condition treatment, payment, enrollment or benefits on a waiver of the right to file a complaint;
10. Implementing and updating policies and procedures on PHI, which are designed to comply with HIPAA;
11. Documentation: A covered entity must:
  - a. Maintain the required policies and procedures in written or electronic form;
  - b. Maintain a written or an electronic copy, as documentation, if a communication is required to be in writing;
  - c. Maintain a written or electronic record of an action, activity, or designation, if the action, activity or designation is required to be documented; and
  - d. Retain the documentation required above for six years from the date of its creation or the date when it last was in effect, whichever is later; and
12. Implementing business associate contracts where required. Business associates are persons to whom a covered entity discloses PHI so that the person can perform a function or activity for the covered entity. There is a separate section in the HIPAA privacy regulations that sets for the requirements for business associate contracts.

### **VIII. ENFORCEMENT OF THE PROPOSED HIPAA PRIVACY REGULATIONS**

The HIPAA privacy regulations contain both civil and criminal penalties. The civil penalties are as follows: \$100 cap per person per violation and \$25,000 cap per person per year for violations of a single calendar year. The criminal penalties include both fines and imprisonment. Criminal fines range from a minimum of \$50,000 to a maximum of \$250,000 and imprisonment ranges from a minimum of 1 year to a maximum of 10 years.

### **IX. CONCLUSION**

The HIPAA privacy regulations have greatly altered the health care system in this country. As a nurse you are faced with PHI information every day and should be familiar with the HIPAA privacy regulations. If you work in a covered entity, a failure to adhere to either the HIPAA privacy regulations or your employer's privacy policies and procedure can result in civil or criminal penalties; furthermore, those penalties can have an effect on you license.

This page intentionally left blank.