

TOPIC ONE

INTRODUCTION AND KEY CONCEPTS

HIPAA and the Privacy Regulations

In 1996, Congress enacted the Health Insurance Portability and Accountability Act, or “HIPAA,” a broad-ranging law that created new federal requirements in many areas of health care. These materials deal with only one aspect of HIPAA – its requirements regarding the privacy of personal health information. Before HIPAA, privacy of medical records and other health-related information was mostly regulated by state law. There were a few federal requirements regarding health information, such as rules about disclosure of alcohol and drug abuse treatment records, but until HIPAA there was no comprehensive scheme of federal regulation in this area.

HIPAA instructed the Secretary of the Department of Health and Human Services to issue regulations regarding privacy of health-related information. Development of those regulations took several years, but they have at last been issued in final form. Entities covered by the regulations are required to be in compliance no later than April 14, 2003.

These materials will familiarize you with the principal requirements of the HIPAA privacy regulations as they affect Maxor and you. This first section will introduce several key concepts that help to define the scope of the requirements imposed by the privacy regulations. Later sections of the materials will cover the circumstances in which an entity may use or disclose health information without the patient’s permission, and when the patient’s permission is required; the rights of patients under the privacy regulations; and the administrative requirements imposed on entities by the regulations.

Key Concepts: Covered Entity

The HIPAA privacy regulations do not apply to everyone. Only certain categories of individuals and businesses are directly regulated by the privacy rules. (Other individuals and businesses may become subject to the regulations indirectly through business associate agreements, which will be covered later.) The regulations use the term “covered entities” to refer to all of the entities to which the rules apply directly. The three categories of covered entities are:

- *Health care providers:* Any health care provider who transmits any health information in electronic form in connection with a “covered transaction” is a covered entity. “Covered transactions” include health care claims, encounter information and referral authorizations, among others. Therefore, a large majority of health care providers are covered entities.

- *Health plans:* Covered entities include any plan that pays the cost of medical care, except for workers compensation plans and a few other specifically excepted kinds of plans. Employer group health plans, health insurance plans, HMOs, Medicare and Medicaid are all covered entities.
- *Health care clearinghouses:* The privacy regulations define a health care clearinghouse as an entity that processes health information received from another entity from a nonstandard format into a standard format, or from a standard format into a nonstandard format. Billing services, repricing companies, community health information systems and value-added networks and switches are all covered entities.

Note that employer-sponsored health plans, including self-insured plans, are covered entities, but employers themselves are not.

Key Concepts: Protected Health Information

The information that is protected by the privacy regulations is referred to as “protected health information,” often abbreviated to “PHI.” PHI includes any information that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and that relates to a person’s physical or mental health or condition; or the provision of health care to a person; or payment for the provision of health care to a person; and that identifies or reasonably could be used to identify the person.

Note that the definition of PHI depends not only on what the information is, but also on who possesses it. Health information is “protected” under the privacy regulations only when it is in the possession of a covered entity. The same information that is PHI when created or received by a covered entity is not PHI if it is collected by a non-covered entity.

Covered entities are required to take steps to protect PHI from unauthorized disclosure, intentional or unintentional. For this reason, it is important to understand just how broad the definition of PHI is. Obviously, medical records and billing records contain PHI and must be kept confidential. But PHI is not only in patient charts, billing systems and claims files, and protecting against unauthorized disclosure of PHI requires much more than just making sure that medical records are kept in a locked room. PHI is on prescription labels, in telephone logs, in customer complaint letters, and on that Post-It note stuck on the side of the computer monitor. When a nurse calls out a patient’s name in the waiting room of a physician’s office, he or she has just disclosed PHI about that patient to everyone in the waiting room. When a pharmacist tells a customer about possible side effects of a drug, and the next person in line overhears the conversation, PHI has been disclosed. PHI is disclosed if a person sees a package left on the next-door neighbor’s doorstep with a return address of “ABC Diabetic Supplies.”

But don't panic. A covered entity is not required to control all disclosures of PHI. These examples are just intended to illustrate how broad the definition of "protected health information" is. The steps a covered entity must take to protect against unauthorized disclosure are covered later in these materials.

Key Concepts: Business Associate

Business associate means a person or entity who performs an activity on behalf of a covered entity, or provides services to or for a covered entity, involving the use or disclosure of protected health information.

Accountants and attorneys, for example, are often business associates of covered entities, because covered entities disclose PHI to them to enable them to perform services for the covered entities. Employees of the covered entity are not considered business associates of the covered entity.

A covered entity is required to have written contracts with its business associates requiring the business associates to safeguard PHI that is disclosed to the business associate against unauthorized use or disclosure, and to cooperate with the covered entity in meeting the covered entity's responsibilities under the privacy regulations.

A covered entity may be a business associate of another covered entity. For example, a billing service may be a covered entity because it may fall within the definition of a health care clearinghouse. However it may also be a business associate of a health care provider, because the provider discloses PHI to the billing company so that the billing company can provide billing services for the provider.

Not all relationships between covered entities and other entities involving disclosure of PHI are business associate relationships. In order for a business associate relationship to be created, one entity must be providing services to, for or on behalf of another entity. For example, when one health care provider refers a patient to another provider, the second provider performs services for the patient, not for the first provider. Therefore, no business associate contract is required.

Note on State Law

HIPAA is a federal law, and applies throughout the United States. However, a special provision of the law states that if a state law imposes requirements that are more stringent – that is, providing more privacy protection, or providing an individual with greater rights regarding his or her own information, or requiring more documentation – than HIPAA or the privacy regulations, then the state law applies. Therefore, the privacy rules establish

a “floor” level of privacy protection, but particular state laws may impose more stringent requirements.

TOPIC TWO

TPO: TREATMENT, PAYMENT AND HEALTH CARE OPERATIONS

Introduction

The privacy regulations state a general rule that a covered entity may not use or disclose PHI without the authorization of the individual who is the subject of the PHI. The regulations then go on to state a number of exceptions to this general rule. Three of the most important of these exceptions relate to core activities of covered entities, which could not practically be conducted if specific authorization were required for every use or disclosure of PHI. Those three exceptions are:

- Authorization is not required for use or disclosure of PHI for purposes of treatment.
- Authorization is not required for use or disclosure of PHI for purposes of payment.
- Authorization is not required for use or disclosure of PHI for purposes of health care operations.

These three exceptions are often thought of as one single broad exception, and are commonly referred to by the single acronym “TPO.” To understand what is and is not permitted under the privacy regulations, you must understand the scope and limitations of the terms “treatment,” “payment” and “health care operations” as defined in the privacy rules.

Treatment

The privacy regulations permit a covered entity to use PHI without the individual’s authorization for purposes of treatment. The regulations define “treatment” as

the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Under this definition, a covered entity may use or disclose PHI without authorization not only for the direct provision of health care treatment, but also for various activities related to the management and coordination of care. For example, when a physician refers a patient to another health care provider, he or she is not required to obtain specific

authorization from the patient to disclose PHI to the other provider to enable the other provider to treat the patient.

→→→ **NOTE:** The privacy regulations deal only with the use of PHI for treatment purposes. This is a separate issue from consent to treatment. The privacy regulations have no effect on legal requirements relating to informed consent to medical treatment.

Payment

Covered entities are not required to obtain the individual's authorization for use of PHI for purposes relating to payment for the individual's treatment. The activities that are covered under the term "payment" as defined in the privacy regulations include not only submission of claims and receipt of payment, but also related activities such as:

- eligibility verification
- precertification
- coordination of benefits
- audit and claims review
- utilization review

Therefore, when a health insurance plan requires precertification for a particular treatment or procedure, a health care provider may disclose PHI to the health plan to obtain precertification without the individual's express authorization.

Health Care Operations

The "O" in TPO stands for "operations." The term "health care operations" is used in the privacy regulations to cover a variety of activities that are not directly related to the treatment of a particular patient, but which require the use of PHI. For example, health care providers review patient records in the course of their quality assessment and improvement activities. PHI is also required for training, credentialing, performance review and compliance activities. The privacy regulations permit covered entities to use PHI for these purposes without the authorization of the individual who is the subject of the PHI.

“Health care operations” also includes certain business planning, management and general administrative activities of the covered entity, but it does not include marketing. In general, covered entities may not use PHI for marketing purposes without the individual’s authorization, subject to certain exceptions that will be covered later in these materials.

The privacy regulations also recognize that PHI must be used and disclosed in connection with the sale or merger of a business, and with the due diligence activities preceding a sale or merger. These activities fall within the definition of “health care operations” as long as the other party to the transaction is also a covered entity, or will become a covered entity following the transaction.

TPO of Other Entities

In some cases, the PHI in the possession of a covered entity is needed for treatment, payment or health care operations of some other entity. For example, an ancillary provider appealing a claim denial may need evidence of medical necessity from the prescribing physician’s medical records. In certain limited circumstances, the privacy regulations permit a covered entity to disclose PHI to another entity for the other entity’s treatment, payment or health care operations purposes. Specifically:

Treatment: A covered entity may disclose PHI to a health care provider for that provider’s treatment activities. This disclosure is permitted whether or not the other provider is a covered entity.

Payment: A covered entity may disclose PHI to another covered entity, or to a health care provider (even if the other provider is not a covered entity), for the covered entity’s or provider’s payment activities.

Operations: A covered entity may disclose PHI to another covered entity (but not to a provider that is not a covered entity) for certain limited health care operations activities of the other entity, but only if the other entity has or had a relationship with the individual who is the subject of the PHI, and the PHI pertains to that relationship. The principal health care operations purposes of another covered entity for which PHI may be disclosed without authorization are:

- > quality assessment and improvement
- > case management and care coordination
- > reviewing the qualifications or evaluating the performance of providers and practitioners

- > training programs
- > accreditation, certification, licensing, or credentialing activities
- > health care fraud and abuse detection and compliance

TOPIC THREE

OTHER USES AND DISCLOSURES OF PHI

Introduction

In addition to uses and disclosures for treatment, payment and health care operations, the privacy regulations permit certain other uses and disclosures of PHI without the individual's express authorization. These uses and disclosures are divided into two categories: those for which the individual must be given an opportunity to object, and those for which an opportunity to object is not required. If a covered entity wishes to use or disclose PHI for any purpose other than the purposes specifically provided for in the privacy regulations, it must obtain the individual's authorization for the use or disclosure.

Uses and Disclosures for Which the Individual Must Be Given an Opportunity to Agree or Object

Persons Involved in Care or Payment. A covered entity may disclose to a relative or close friend of the individual, or any other person identified by the individual, PHI that is directly relevant to that person's involvement with the individual's care or payment for that care, subject to the conditions described below. A covered entity may also use or disclose PHI protected health information to notify a family member, personal representative, or other person responsible for the individual's care of the individual's location, general condition, or death.

If the individual is present or available and has the capacity to make health care decisions, the covered entity may use or disclose the PHI if (1) it provides the individual with the opportunity to agree or object to the disclosure, and the individual agrees or does not object, or if (2) it reasonably infers from the circumstances that the individual does not object to the disclosure.

If the individual is not present or available, or does not have capacity to make health care decisions, or if an emergency makes it impractical to provide the opportunity to object, then the covered entity may disclose PHI that is directly relevant to the person's involvement with the individual's health care if it reasonably determines that the disclosure is in the best interests of the individual.

This exception makes it possible for a relative or friend to pick up a prescription for a patient, even though the pharmacy is disclosing PHI about the patient to the relative or friend by delivering the prescription.

Uses and Disclosures for Which an Opportunity to Object Is Not Required

Incidental Uses and Disclosures. Uses and disclosures of PHI that are “incidental” to otherwise permitted uses and disclosures do not violate the privacy rules as long as the covered entity has reasonable safeguards in place to protect the privacy of PHI, and is in compliance with the other provisions of the privacy rules. For example, if a conversation between a pharmacist and a patient is overheard by someone in a waiting room, that disclosure does not violate the privacy rules if the pharmacist has taken reasonable precautions to avoid being overheard. If a person standing in line at a pharmacy counter happens to see the label on a prescription bottle as it is handed to a customer, the disclosure would be incidental and would ordinarily not be considered a HIPAA violation. However, if the pharmacist discusses a customer’s medical condition in a loud voice when other customers are clearly within hearing range, he or she would not be considered to have taken reasonable precautions to avoid being overheard, and the disclosure would not be protected by the “incidental” exception.

Disclosures Required by Law. Various disclosures that are required by law do not require the individual’s authorization. These include reporting of certain diseases, reports concerning victims of abuse, and disclosures in response to court orders. PHI may be disclosed in response to a subpoena if the subpoena is accompanied by a court order. However, a covered entity may not disclose PHI in response to a subpoena that is not accompanied by a court order unless it receives assurance that certain protective steps have been taken.

Public Health and Health Oversight Activities. A covered entity may disclose PHI without the individual’s authorization to entities that conduct certain public health activities, such as public health surveillance, disease and vital event reporting, and FDA product tracking and post-marketing surveillance. A covered entity may also disclose PHI for “health oversight activities,” including Medicare and Medicaid audits, licensure actions, and civil and criminal investigations. However, this exception does not apply if the individual is the subject of the investigation or activity and the investigation or activity is not directly related to health care or public benefits related to health.

Other Disclosures. Other disclosures that are permitted without the authorization of the individual include:

- Disclosures to coroners, medical examiners and funeral directors as necessary to enable them to carry out their duties
- Disclosures to organ procurement organizations
- Certain disclosures for research purposes, if the research is approved by an Institutional Review Board or privacy board and meets certain other requirements

- Disclosures required for workers compensation programs

Uses and Disclosures Requiring Authorization

If a covered entity wishes to use or disclose PHI for any purpose other than the purposes specifically permitted by the privacy regulations, it must obtain an authorization from the individual who is the subject of the PHI. In particular, a covered entity must obtain the individual's authorization to use or disclose PHI for purposes of marketing. The marketing provisions of the privacy rules are complex and not entirely clear, and may be subject to change. In general, however, the rules define marketing to include any communication about a product or service that encourages recipients to purchase or use the product or service, except for communications for treatment or case management purposes, and except for certain communications describing health-related products or services of the covered entity. The only marketing uses of PHI that do not require authorization are face-to-face communications and promotional gifts of nominal value.

Requirements for a valid authorization are covered in the next topic.

TOPIC FOUR

AUTHORIZATIONS

Introduction

As discussed in the previous topic, the privacy regulations require a covered entity to obtain the individual's authorization for any use or disclosure of PHI other than those uses and disclosures specifically permitted by the rules. This topic covers the requirements for a valid authorization, and other issues related to authorizations.

Requirements for a Valid Authorization

An authorization must be in writing and must be signed by the individual. It must be written in plain language, and a copy must be provided to the individual. The authorization must contain the following:

- A specific description of the information to be used or disclosed.
- Identification of the persons authorized to make the requested use or disclosure.
- Identification of the persons to whom the covered entity may make the requested use or disclosure.
- A description of the purpose of the requested use or disclosure. If the individual requests the disclosure, the description may just state "at the request of the individual."
- An expiration date or an expiration event.
- The signature of the individual and the date. If the authorization is signed by a personal representative of the individual, a description of the representative's authority to act for the individual must also be provided.
- Statements clearly informing the individual of:
 - The individual's right to revoke the authorization in writing, the exceptions to the right to revoke and a description of how the individual may revoke the authorization. If this information is included in the covered entity's Notice of Uses, the authorization may just refer to the Notice. (The Notice of Uses is covered in a later topic.)

- The fact that the covered entity may not require the individual to sign the authorization as a condition to providing treatment, payment, enrollment or eligibility for benefits, or the consequences of not signing the authorization if an exception to this rule applies.
- The fact that information disclosed could be subject to redisclosure by the recipient and no longer be protected by the privacy regulations.

An authorization for use or disclosure of PHI may not be combined with another document such as a consent to treatment or an assignment of benefits.

Authorization as a Condition of Treatment

A covered entity may not make the signing of an authorization a precondition to obtaining treatment, payment, enrollment or eligibility for benefits. There are a few exceptions to this rule, but they are quite limited and generally not applicable to Maxor. For example, research-related treatment may be conditioned on an authorization for use of PHI for purposes of the research.

Revocation of Authorization

An individual may revoke an authorization at any time, except to the extent that the covered entity has acted in reliance on the authorization. A revocation must be in writing.

TOPIC FIVE

BUSINESS ASSOCIATES

Introduction

Covered entities often engage other entities to perform healthcare-related activities and functions on their behalf that require use or disclosure of PHI. The privacy regulations refer to these entities as business associates. Business associates include entities that provide claims processing, quality assurance, billing and practice management. Entities providing legal, accounting, financial or administrative services to a covered entity may also be business associates, if the provision of such services involves use or disclosure of PHI.

Not all relationships between covered entities and other entities that involve use or disclosure of PHI are business associate relationships. When a provider participates in a health plan's network, the provider and the plan must exchange PHI, but they are not necessarily business associates. In order for a business associate relationship to exist, one entity must be providing services or performing functions to or on behalf of the other entity. In a simple payor-provider relationship, neither entity is providing services to or on behalf of the other. Similarly, when one provider refers a patient to another provider, no business associate relationship is created unless one is performing services for or on behalf of the other.

Business Associate Agreements

The regulations permit a covered entity to release PHI to a business associate to enable the business associate to carry out functions on behalf of the covered entity. However, the covered entity must obtain assurances that the business associate will safeguard the PHI disclosed to it from misuse, and that it will help the covered entity comply with the covered entity's responsibilities with respect to PHI. This is generally accomplished through the use of a contract called a business associate agreement. A business associate agreement specifies the permitted and required uses and disclosures of PHI by the business associate, provides that the business associate will not use or disclose PHI other than as permitted by contract and required by law, and requires the business associate to use appropriate safeguards to prevent unauthorized uses or disclosures. It also requires the business associate to make an individual's PHI available if the individual requests it and to make available information required for the covered entity to comply with the regulations.

Responsibilities of Covered Entities

A covered entity is not required to actively monitor or oversee the means by which the business associate safeguards PHI or the extent to which the business associate abides by the requirements of the business associate agreement. A violation by the business associate is not in and of itself a violation of the HIPAA regulations by the covered entity. However, if a covered entity becomes aware of a practice by the business associate that is a breach of the business associate's obligations, the covered entity must take reasonable steps to cure the breach or the covered entity must end the relationship.

Covered Entities as Business Associates

Being a business associate of a covered entity does not, in itself, make the business associate a covered entity under the privacy regulations. For example, an accounting firm or a transcription service does not become a covered entity by entering into a business associate agreement with a covered entity. Accounting firms and transcription services are not directly covered under the privacy regulations, and are bound by those regulations only through the business associate agreement. (However, these entities may be covered by state privacy laws.)

However, some business associates of covered entities are also covered entities themselves. A health care clearinghouse, for example, is a covered entity, and may also be a business associate of many other covered entities. A covered entity that is acting as a business associate of another covered entity is bound both by the business associate agreement and by the privacy rules directly. If it violates the assurances it has given the other covered entity in its business associate agreement, is considered to be violating the privacy regulations.

TOPIC SIX

THE “MINIMUM NECESSARY” STANDARD

Introduction

In addition to prescribing when a covered entity may use or disclose PHI, the privacy regulations also specify how much PHI the entity may use or disclose. The general rule is that use or disclosure of PHI must be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure. The same standard applies to requests by a covered entity for disclosure of PHI from another covered entity.

Uses and Disclosures to Which the Minimum Necessary Standard Applies

In general, a covered entity must make reasonable efforts to limit protected health information that it uses, discloses or requests from another covered entity to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. However, the minimum necessary standard does not apply to the following uses and disclosures:

- Disclosures to or requests by a health care provider for treatment
- Uses or disclosures made to the individual
- Uses or disclosures made pursuant to an authorization
- Disclosures made to the Secretary of Health and Human Services as required under the privacy rules
- Uses or disclosures that are required by law
- Uses or disclosures that are required for compliance with the privacy rules

Employee Access to PHI

The minimum necessary standard applies to use of PHI within the covered entity as well as to disclosures to other persons or entities. Therefore, the covered entity must restrict access to PHI among its own employees as well as release of PHI outside the organization. A covered entity is required to identify the members of its workforce who need access to PHI to carry out their duties, and the category or categories of PHI to which each person or category of persons needs access. The covered entity must make

reasonable efforts to limit each person's access to PHI to the information he or she needs to perform his or her job.

Request for or Disclosure of Entire Medical Record

Before the issuance of the privacy regulations, it was routine for health care providers, third-party payors, attorneys and others to request and receive copies of entire medical records, even if only a portion of the record was relevant to the purpose of the request. The privacy regulations specifically provide that except for uses, disclosures and requests to which the minimum necessary standard does not apply, a covered entity may not use, disclose or request an entire medical record, unless the entire medical record necessary to accomplish the purpose of the use, disclosure, or request.

TOPIC SEVEN

NOTICE OF USES

Introduction

Individuals have the right under the privacy rules to receive a written notice of the uses and disclosures of their PHI that might be made by a covered entity, and of the individual's rights and the covered entity's duties with respect to PHI. Each covered entity must prepare such a notice and make it available as provided in the regulations.

Content of the Notice of Uses

Some of the elements required to be included in a Notice of Uses are:

- A description of the types of uses and disclosures that the covered entity is permitted to make for treatment, payment, and health care operations, including at least one example of each.
- A description of each of the other purposes for which the covered entity is permitted to use or disclose PHI without the individual's authorization.
- A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke the authorization.
- A statement of the individual's rights with respect to PHI and how the individual may exercise those rights.
- A statement that the covered entity is required by law to maintain the privacy of PHI, to provide individuals with its Notice of Uses, and to abide by the terms of its Notice of Uses currently in effect.
- A description of how the individual may file a complaint regarding a violation of his or her privacy rights.

Delivery of the Notice of Uses

The requirements for making the Notice of Uses available to individuals vary according to the type of covered entity.

If the covered entity is a health care provider, it must provide the Notice of Uses to any individual with whom it has a direct treatment relationship on the first date of service after April 14, 2003 or, in the case of emergency treatment, as soon as is practicable. A health care provider must also make a good faith effort to obtain a written acknowledgment of the individual's receipt of the Notice of Uses. If the covered entity is not able to obtain a signed acknowledgment, it must document its good faith efforts and the reason the acknowledgment was not obtained. If the provider maintains a retail location or physical service site, the provider must have the Notice of Uses available to any individual who requests a copy, and must post the Notice of Uses in a clear and prominent location.

Health care clearinghouses are not required to provide copies of the Notice of Uses to all individuals whose PHI they maintain, but they must make the Notice available on request.

Any covered entity that maintains a web site must prominently post its Notice of Uses on the web site and make it available electronically through its web site.

An entity that is a business associate of a covered entity, but that is not a covered entity itself, is not required to have a Notice of Uses.

Revisions to the Notice of Uses

Whenever a covered entity makes changes in its privacy practices, it must revise the Notice of Uses and make the revised Notice available. Health care providers are not required to distribute the Notice to all of their patients every time it is revised, but they must post the revised Notice and make copies available on request.

TOPIC EIGHT

RIGHTS OF INDIVIDUALS

Introduction

Individuals have several specific rights in relation to their PHI under the privacy regulations. These include:

- The right to receive written notice of the covered entity's privacy practices, and the individual's rights with respect to PHI.
- The right to have access to, and obtain a copy of, the individual's PHI.
- The right to receive an accounting of disclosures of the individual's PHI.
- The right to request correction and/or amendment of the individual's PHI.
- The right to request restrictions on the use and disclosure of the individual's PHI.

Right to Receive Notice of Privacy Practices

Individuals have the right under the privacy rules to receive written notice of the covered entity's privacy practices, and of the individual's rights with respect to PHI. This is the Notice of Uses that was covered in Topic Seven.

Right of Access to PHI

A covered entity must permit an individual access to his PHI in order for the individual to inspect and to obtain a copy of PHI about the individual that the covered entity maintains. If an individual requests access to his or her PHI, the covered entity must act on the request within thirty days. The covered entity may deny access under certain circumstances. For example, access may be denied if the PHI was compiled for use in a civil, criminal or administrative action or proceeding, or if a licensed health care professional determines that granting access is reasonably likely to cause harm to or endanger the life or safety of the individual or another person. In some cases the individual has a right to an independent review of a denial of access.

If the individual requests a copy of the PHI, the covered entity may impose a reasonable, cost-based fee, which may include only the cost of copying, plus postage if the individual requests that the copies be mailed.

Right to an Accounting of Disclosures

An individual has the right to request and receive an accounting for disclosures of PHI made by a covered entity (or by business associates of the covered entity) for up to six years prior to the date of the request. Therefore, a covered entity must track and document disclosures of PHI in order to be able to respond to a request for an accounting. However, this requirement is not as burdensome as it sounds, because the accounting is not required to include:

- Disclosures for purposes of treatment, payment and health care operations.
- Disclosures to the individual himself or herself, or disclosures for which the individual signed an authorization.
- Disclosures to persons involved in the individual's care as provided by the regulations.
- Disclosures that are incidental to other permitted disclosures.
- Disclosures that occurred prior to April 14, 2003.

For all other disclosures, the accounting must include the date of the disclosure, a description of the PHI disclosed, the entity or person who received the PHI, and the purpose of the disclosure.

A covered entity must act on a request for an accounting within sixty days after receiving the request. The first accounting to an individual in any twelve-month period must be provided without charge. The covered entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the twelve-month period.

Right to Request Correction or Amendment

An individual may request that a covered entity amend PHI maintained by the covered entity. A covered entity may deny an individual's request for amendment if it determines that the PHI is accurate and complete. A covered entity may also deny a request if the PHI not created by the covered entity, unless the individual shows that the originator of PHI is no longer available to act on the requested amendment.

A covered entity must act upon a request for amendment within sixty days. If the covered entity agrees to amend its records, it must make reasonable efforts to notify business associates and others that have the PHI that is the subject of the amendment. If

a covered entity is informed by another covered entity of an amendment to an individual's PHI, the covered entity must amend the PHI it maintains.

If the covered entity denies the request for an amendment, it must provide the individual with a written denial stating the basis for the denial. It must also permit the individual to submit a written statement disagreeing with the denial. If the individual submits a statement of disagreement, the covered entity must include that statement with any future disclosures of the affected PHI. Even if the individual does not submit a statement of disagreement, he or she may request that the covered entity include the request for amendment (or a summary of the request) and its denial with any future disclosures.

Right to Request Restrictions

An individual may request that a covered entity observe additional restrictions on its uses and disclosure of PHI, beyond the restrictions imposed by the privacy regulations. The covered entity is not required to agree to additional restrictions. However, if it does agree to additional restrictions, the covered entity may not disclose or use PHI in violation of those restrictions.

TOPIC NINE

VIOLATIONS, PENALTIES AND SANCTIONS

The HIPAA statute imposes both civil and criminal penalties for violations. The Secretary of Health and Human Services may impose civil penalties of \$100 for each violation, up to a total of \$25,000 per year. The possible criminal penalties are more severe. A person who knowingly obtains or discloses PHI in violation of the privacy rules may be fined up to \$50,000 and imprisoned for up to a year. If the offense is committed under false pretenses, the fine may be up to \$100,000, and imprisonment may be up to five years. And a person who commits an offense with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, may be fined up to \$250,000 and imprisoned for up to ten years.

The privacy rules require that a covered entity sanction members of its workforce who fail to comply with the privacy regulations or with the entity's privacy policies. Any Maxor employee who fails to comply with the privacy regulations or with Maxor's policies and procedures will be subject to disciplinary measures up to and including termination of employment.