

HIPAA:

Health Information Compliance

2001

Compliance Deadline:
April 2003

TABLE OF CONTENTS

OVERVIEW OF HIPAA, TRANSACTION AND CODE SET STANDARDS	Section 1
THE PRIVACY RULES USE AND DISCLOSURE	Section 2
THE PRIVACY RULES: RIGHTS OF THE PATIENT	Section 3
THE PRIVACY RULES: ORGANIZATIONAL REQUIREMENTS	Section 4
ORGANIZATIONAL TASKS	Section 5

SECTION 1

OVERVIEW OF HIPAA TRANSACTION AND CODE SET STANDARDS

AN OVERVIEW OF HIPAA

1. What is HIPAA?

HIIPAA stands for the Health Insurance Portability and Accountability Act of 1996 (PL 104-91)

2. Why was HIPAA enacted?

The purpose of the Act, according to the introductory paragraph, is to:

"...improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

3. History of HIPAA. There are five top-level titles of the Act:

- a. Title I: Healthcare Access, Portability, and Renew ability
Eliminated pre-existing condition exclusions
Prohibits discrimination based on health status
Guarantees coverage renewal
- b. Title II: Preventing Healthcare Fraud and Abuse; Administrative Simplifications, Medical Liability Reform
- c. Title III: Tax-Related Health Provisions
- d. Title IV: Applications and Enforcement of Group Health Requirements
- e. Title V: Revenue Offsets

4. Today's focus: The two words highlighted above: simplify administration, or as it's been restated: Administrative Simplification. This includes:

- a. Standards governing the electronic transmission of certain administrative and financial transactions
- b. Standards protecting the Privacy of all electronically-maintained, individually identifiable health information (the major portion of our day today)
- c. Security of the same information above (which is different than Privacy, and rules are not yet final)

5. What is the definition of health information?

Health information (oral or written) in any form or medium that:

Is created by a health care provider, health plan, public health care authority, employer, life insurance company, school, university or health care clearing house, AND

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.

6. What is individually identifiable health information? Health information that identifies an individual, OR creates a reasonable basis from which to believe that the information can be used to identify an individual

7. What are the penalties for non-compliance with these rules?

- a. **Monetary penalties:** Each violation is punishable by a fine of up to \$100, not to exceed \$25,000 in a calendar year for identical violations
- b. **Criminal penalties:** For knowingly obtaining or disclosing individually identifiable health information:

A fine of not more than \$50,000, imprisonment for not more than one year, or both. If committed under false pretenses, a fine of not more than \$100,000, imprisonment for not more than 5 years, or both. If committed with intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm, a fine of not more than \$250,000, imprisonment of not more than 10 years, or both.

TRANSACTION STANDARDS

1. Why were national electronic standards proposed?

Administrative simplification: To achieve administrative savings and reduce the administrative burden on health care providers and health plans.

To reduce the multiplicity of different formats

2. What does a national standard for electronic transactions mean?

It means one format, standard content, and automatic acceptance by health plans.

3. When must I comply with these electronic standards?

The compliance date for the Transaction and Code Sets Final Rule is October 17, 2002.

CODE SET STANDARDS

1. What is a “Code Set”?

Any set of codes used for encoding data elements, such as tables of terms, medical concepts, medical diagnosis codes or medical procedure codes.

Examples: ICD-9-CM, CPTA, and HCPCS

2. What Code Sets are recommended in the Rule? Those above (I)

ICD-9-CM: Used for all inpatient diagnosis and procedure coding for administrative transactions (and probably will transition to ICD- 10)

CPT-4: Used for outpatient procedure coding and physician services

HCPCS: Used in ambulatory settings for medical equipment, injectable drugs, transportation services, and other services found in CPT-4.

CDT-2: Used for reporting dental services

NDC: Used for reporting prescription drugs in pharmacy transactions and some claims by health professionals

3. Who needs to pay attention to this?

Those who produce and/or process electronic health transactions should begin preparing for system changes to allow for these regulations.

NATIONAL IDENTIFIERS

1. What unique health identifiers are required by HPA?

- a. Individuals: Much public comment has halted forward movement on a national identifier for individuals. Only specific legislation approving such a standard will set it in motion again. There is much concern about the ease of access to private information by a single identifier.
- b. Employers: Likely to be 2003. The proposed rules recommend use of the Employer Identification Number (EIN) assigned by the IRS. HPA does not require that employers use the EIN for standard health care transactions. Providers, health plans, and clearing houses are required to use the identifier in electronic transactions.
- c. Health Plans or Payers: Date not set for implementation. Likely to be the 9 digit number assigned to all health plans.

2. Provider Identifiers: Probably will be a new, unique identification number called the National Provider Identifier (NPI) for all health care providers.

Why spend the money to set up a totally new system'?

- a. Each provider should have only one identifier
- b. Must be comprehensive, accommodating all provider types, with ability to be valid for years to come, accommodate 100 million entities
- c. Must be confidential and private
- d. Must be intelligence-free

3. Proposed National Provider File

- a. Would collect and store information about a health care provider
- b. License
- c. Location of provider
- d. Membership in groups
- e. Estimated cost of Provider File set up: \$50 per provider

4. Who would have access to such a file?

- * Enumerators
- * Public

SECTION 2

THE PRIVACY RULES USE AND DISCLOSURE

THE PRIVACY RULES: USE AND DISCLOSURE

Part I: Introduction

A. Who is affected?

1. Healthcare providers
 - a. Direct Relationship (Doctor, Physical therapist, PA, Nurse, etc...)
 - b. Indirect Relationship (Radiologist, Pathologist, etc...)
2. Healthcare clearinghouses (Billing service, Community Health, coding, etc...)
 - a. Types
 - b. Role
3. Health plans
4. Business Associates (Check all contracts ie. "Craig's Office Supply")

B. Selected Definitions

1. **Designated Record Set**
 - a. A group of records that is the medical records and billing
 - b. Enrollment, payment, claims adjudication
 - c. Used by the entity to make decisions
2. **Entity:** the health care provider (covered entity), plan, clearinghouse
3. **Disclosure:** Release of information outside the entity
4. **Healthcare Operations:**
 - a. QM
 - b. Reviewing/evaluating practitioners
 - c. Underwriting, premium rating
 - d. Medical review, legal services, auditing
 - e. Business planning/development
 - f. General administrative (complaints, grievances, customer service)
5. **Individual:** person who is the subject of PHI
6. **PHI:** Protected Health Information, identifiable health information that is:
 - a. Transmitted by electronic media
 - b. Maintained in any medium
7. **Use:** the sharing, employment, application, utilization, examination or analysis of the information within an entity that maintains such information
8. **Workforce:** employees, volunteers, trainees, and other persons whose conduct in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Part II: Consent to Carry Out Treatment, Payment or Health Care Operations

A. Minimum Necessary (164.502(b))

1. **Definition:** An entity must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose or use, disclosure or request.
2. **Minimum Necessary does not apply to:**
 - a. Disclosure to a provider for treatment purposes
 - b. The individual
 - c. DHHS who may have any information to investigate or determine compliance
 - d. Uses/disclosures required by law
3. **Workforce identification:** (164.514 (d)(2))
 - a. Entity must identify employees (or classes of) who need access to PHI to carry out their duties
 - b. And, identify the categories of PHI to which access is needed (Policies and Procedures)
4. **Policies and Procedures** (164.514(d)(3))
 - a. Entity must develop and implement reasonable policies and procedures that limit the PHI disclosed on a "routine and recurring" basis to what is necessary
 - b. Develop reasonable criteria to review requests
5. **Entity is permitted to assume that a request is for the minimum necessary information when** (164.514(d)(3))
 - a. Making disclosures to public official
 - b. The request is from another covered entity
 - c. Requested by a member of its workforce or is a Business Associate (BA) if it is represented that the information requested is minimum necessary
6. **Requesting Information:** A covered entity must limit its own requests for PHI to what is reasonably necessary to accomplish the purpose.
7. **Entire Record:** A covered entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. (164.514(d)(5))

B. Consent for Use (Treatment, Payment, or Health Care Operations)

1. Entity must obtain consent from the individual in order to use or disclose PHI for treatment, payment or health care operations. (164.506(a))
2. Routine Use includes:
 - a. Disclosure to other providers for consultation
 - b. Disclosure as part of referrals
 - c. Use for payment purposes
 - d. Use for healthcare operations
3. Exceptions (164.506(a)(2))
 - a. There is an indirect treatment relationship
 - b. The individual is an inmate
 - c. In emergency situations
 - d. The entity is required by law to treat
 - e. There are substantial barriers to communicating

4. Failure to obtain consent must be documented
5. Treatment may be conditioned upon consent (164.506(b))
6. A consent for use or disclosure may be combined with other consents if it is visually separate from the other consent, and signed separately. (164.506(b)(4))
7. Consent may be revoked, except to the extent that the covered entity has taken action in reliance upon the consent.
8. It may not be combined with the Notice of Privacy

C. Elements of a valid consent for use (164.506(c))

1. It must be in plain language
2. It must inform the individual that PHI may be used and disclosed to carry out treatment, payment or healthcare operations;
3. Refer the individual to the Notice of Privacy for a more complete description of such uses and disclosures
4. Must state that the individual has the right to request that the covered entity restrict how PHI is used or disclosed to carry out treatment, payment, or healthcare operations, although the covered entity is not required to agree to requested restrictions
5. Must state that the individual has the right to revoke the consent in writing, except to the extent the entity has taken action
6. Must be signed and dated by the individual

D. Defective Consents: There is no consent if the document has the following defects:

1. It lacks an element above, or
2. It has been revoked

E. Conflicting Consents and Authorizations

1. If there are two consents/authorizations, the more restrictive consent/authorization applies.
2. The covered entity may try to resolve the conflict.

F. Joint Consents

1. Entities who participate in an organized healthcare arrangement and have a joint notice under the Rule's Notice of Privacy Practices may use a joint consent.
2. Joint Consent must include:
 - a. Specific identities of the covered entities, or classes of the covered entities
 - b. Meet all the other requirements for a valid consent
 - c. If the individual revokes a joint consent, the entity that receives it must inform the other entities.

Part IV: Uses and Disclosures Needing Authorization

A. General Rule: An entity may not use or disclose PHI without an authorization that is valid

B. Psychotherapy notes: An entity must obtain authorization for the use of psychotherapy notes except:

1. To carry out treatment by the originator of the notes
2. Use by entity in training programs for students in mental health under supervision learning to practice
3. Use by entity to defend a legal action brought by the individual

C. Elements of a Valid Authorization: In Plain Language (164.508(b-c))

1. A description of the information to be used or disclosed that identifies the information in a meaningful fashion.
2. Name of person or class of persons authorized to make the specific disclosure
3. Name, specific identification, or class of persons getting the information
4. An expiration date or event that relates to the individual or purpose of the use/disclosure
5. A statement of the individual's right to revoke the authorization in writing, and how to do so
6. A statement that information disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by this rule
7. Signature of the individual and date
8. If signed by a personal representative, a description of their legal authority

D. Authorizations requested by entity for own use or disclosure

1. In addition to above, it must contain:
 - a. A statement that the entity will not condition treatment, payment, etc on the authorization
 - b. A description of each purpose of the use
 - c. A statement that the individual may inspect or copy and
 - d. A statement the individual may refuse to sign the. authorization
2. The individual must get a copy of the authorization

E. Authorizations requested by an entity for disclosures by others. If an entity requests an authorization for another entity to disclose PHI to the first entity in order to carry out treatment, payment, or health care operations, the entity requesting must comply with the following:

1. In addition to C above, it must have
 - a. A description of each purpose of the requested disclosure
 - b. A statement that the covered entity will not condition treatment
 - c. A statement that the individual may refuse to sign the authorization
2. The individual must get a copy of the authorization

F. Research including treatment of the individual (164.508(f))

1. An authorization for use and disclosure of PHI must contain
 - a. For use and disclosure not permitted or required, meet the requirements of C and D above,
 - b. A description of how PHI will be used
 - c. A description of any PHI that will not be used for purposes permitted

- d. A statement referring to the consent for use, if obtained, and the notice of privacy practices
2. Optionally, the authorization may be in the same document as the consent to participate in the research, consent to use or disclose PHI to carry out treatment, payment or healthcare operations, or a notice of privacy practices.

G. Valid Authorizations (164.508(b)(2))

1. A valid authorization must have minimally the elements listed above. It may contain information in addition to those required, provided it is not inconsistent with the required elements
2. It is not valid if any elements are missing or not filled out
3. It is not valid if the expiration date has passed
4. It is not valid if known to be revoked
5. if elements provided are known to be false

H. Compound Authorizations. Authorizations for use or disclosure of PHI may not be combined with any other document, except: (164.508(b)(3))

1. Use and disclosure for research combined with treatment authorization
2. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes
3. Authorizations for multiple uses of PHI may be combined only if the entity has not conditioned the provision of treatment, payment, etc. on the provision of one of the authorizations

I. Exceptions to Prohibition on Conditioning of Authorizations (164.508(b)(4))

1. Research may be conditioned on authorization
2. Enrollment in a health plan or eligibility of benefits (except for psychotherapy notes)
3. Disclosure is necessary to determine payment and the authorization is not for psychotherapy notes

J. Revocation and Documentation (164.510(a))

1. An individual may revoke in writing at any time, except for previously mentioned exceptions
2. Signed authorizations must be retained

Part V: Uses and Disclosures Requiring an Opportunity for the Individual to Object (may be oral)

A. Facility Directories

1. Permitted use
 - a. Name
 - b. Location in Facility
 - c. Condition
 - d. Religious affiliation
2. Disclose such information to
 - a. Members of the clergy
 - b. Others who ask, by name, except for religious information
3. Opportunity to object: Individual has right to be informed of directory and have opportunity to restrict or prohibit some or all information
4. Emergencies: information may be disclosed if it is consistent with known preferences and in the best interest of the individual determined by the provider

B. Use and Disclosure for involvement in the individual's care and notification purposes (164.510(b))

1. Permitted uses:
 - a. Family member, other relative or close personal friend PHI relevant to such person's involvement with the individual
 - b. For notification of family member etc re: condition, location, or death
2. Use and Disclosure with the Individual present: may do so if:
 - a. Obtains individual's agreement
 - b. Provides the individual with opportunity to object to the disclosure, and he does not object
 - c. Reasonably infers from the circumstances that the individual does not object
3. Limited Use and Disclosure when the individual is not present
 - a. Individual's best interest
 - b. Directly relevant information
4. Disaster Relief

Part VI: when an Authorization is Not Required

A. When it is required by law

B. Public Health Activities

1. May be disclosed for public health activities to:
 - a. Prevent disease, injury, disability, births, deaths, etc
 - b. Report child abuse or neglect
 - c. FDA
 - d. Report communicable disease
 - e. Employer, re employee, if:
 1. There is workplace health care provider
 2. Concerning work related illness
 3. Needs for legal obligations of employer
 4. Notice is provided to employee that work related PHI is provided

C. Permitted Uses: If entity is Public Health authority, may use PHI in all cases in which it is permitted to disclose such information for Public Health activities.

D. Disclosures re: victims of abuse, neglect, domestic violence

1. Entity may disclose to agencies authorize to receive such information
 - a. To the extent it is required by and complies with law
 - b. If individual agrees to disclosure, or
 - c. If statute or regulation expressly authorizes disclosure
2. The individual must be informed of the disclosure, except if
 - a. It would place the individual at risk of serious harm
 - b. The entity is informing a personal representative, who entity believes is responsible for the abuse

E. Health Oversight Activities (164.512(d))

1. Disclosures are permitted to health oversight agencies for activities authorized by law (audits, civil, criminal & administrative investigations, inspections, licensure or disciplinary actions) for oversight of
 - a. The health care system
 - b. Government benefit systems when relevant
 - c. Government regulatory programs for compliance
 - d. Civil rights compliance
2. Exception: When the investigation is regarding the individual and is not related to health care, public benefits, or qualification of public benefits.

F. Disclosures for Judicial and Administrative Proceedings.

Entity may disclose PHI:

1. In response to a court order (164.512(e))
2. In response to a subpoena, if the proper procedures were followed in notification of the individual of the subpoena, and the individual does not object.
3. In response to a subpoena, and entity makes sufficient effort to notify individual.

G. Disclosures for law enforcement purposes. Entity may disclose PHI:

1. As required by law (certain types of wounds, or other injuries, except those requiring reporting to special agencies)
2. In compliance with the legal process (E above)
3. As limited information for identification and location purposes (identity a suspect, fugitive, witness), only the following:
 - a. Name and address
 - b. Date and place of birth
 - c. SS#
 - d. ABO blood type, rh factor
 - e. Type of injury
 - f. Date and time of treatment
 - g. Date and time of death
 - h. Distinguishing physical characteristics
4. May not disclose info related to DNA or analysis, dental records, or body fluid analysis
5. Crime victims
 - a. The individual agrees to disclosure, or
 - b. Determination of a crime
 - c. No time to get agreement
 - d. In best interests of the victim
6. May alert law enforcement of a death, if there is suspicion it resulted from criminal activity.
7. Crime on the premises (must be good faith belief)

H. Uses and Disclosures about Decedents

1. May disclose to coroner to identify body, cause of death or other duties as required by law
2. To funeral directors, as necessary to carry out their duties
3. To organ procurement organizations for transplants, etc

I. Research. (164.512(i))

1. A covered entity may disclose PHI for research, provided that:
 - a. The patient has authorized the use through a properly authorized consent form approved by an 'RB, or
 - b. A privacy board has approved the waiver
2. Prior to research, obtains from the researcher necessary assurances

J. Uses and disclosures to avert a serious threat to safety (164.512(j))

1. Necessary to lessen or prevent a serious threat, made to an appropriate person
2. To identify or apprehend an individual

K. Military and Federal Government

L. Correctional Facilities

1. Entity may disclose to a correctional institution or law enforcement official who has custody of an inmate.
2. There is no application after release.

PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION: DE-IDENTIFICATION

A. Definition: Health information that does not identify an individual and that there is no reason to believe the information can be used to identify an individual is considered not individually identifiable information. (164.514(a-c))

B. Requirements for de-identification: The following information is removed from the information:

1. Names
2. Geographic identifiers
 - a. Subdivisions smaller than state
 - b. Street addresses
 - c. City
 - d. County
 - e. Precinct
3. Zip Code: at any level less than the initial three digits (unless the area is 20,000 people)
4. All elements of dates (except year)
5. Telephone numbers
6. Fax numbers
7. Email addresses
8. SS#
9. Medical Record Numbers
10. Health plan beneficiary numbers
11. Account Numbers
12. Certificate/License numbers
13. Vehicle identification numbers
14. Device identifiers and serial numbers
15. URLs
16. IO addresses
17. Biometric identifiers
18. Full face photographic images
19. ANY unique identifying number
20. Once removed, the entity must attest it has no knowledge that the information could be used to identify a subject of information

C. Alternative Process: Evaluation by statistical expert

D. Re-identification: An entity may assign a code or other means of record identification to allow information de-identified to be re-identified, provided that:

1. Derivation is not used
2. Security of information is established

SECTION 3

THE PRIVACY RULES

RIGHTS OF THE PATIENT

RIGHTS OF THE PATIENT

Right of an Individual to Request Restriction of Uses and Disclosures of PHI (164.522(a))

1. A covered entity must permit an individual to request that the entity restrict uses and disclosures of PHI about the individual to carry out treatment, payment, or health care operations, and disclosures related to involvement in an individual's care.
2. The covered entity is not required to agree to the restriction
3. If the entity agrees to the restriction, it must document and comply with the restriction, unless an emergency compels the release or use of the PHI.
4. The restriction can be terminated if agreed to by the individual and documented (or oral discussion is documented), or the covered entity informs the individual

Access of Individuals to Protected Health Information

1. An individual has the right of access to inspect and obtain a copy of PHI maintained in the record set, except for:
 - a. Psychotherapy notes
 - b. Information compiled in anticipation of or for use in an action/proceeding
 - c. PHI maintained by an entity subject to CLIA
2. The entity may deny the individual access without providing an opportunity for review, in the following circumstances:
 - a. The entity is a correctional institution, or provider acting under the direction of the institution, and if providing access would jeopardize the health, safety, etc. of the individual or other inmates, the safety of any officer, etc.
 - b. The information is created in the course of research, and the individual agreed to a temporary restriction of access when consenting to participate in the research
 - c. The information was obtained from someone other than a health care provider under a promise of confidentiality and the access would reveal the source.
3. The entity may deny the individual access, but the individual is given a right to have such denial reviewed. The review is by a health care professional designated by the entity to act as reviewing official, and did not participate in the original decision to deny. The reviewing official must determine within a reasonable period of time, whether or not to deny the access requested based on the standards.

4. The entity must permit the individual to request access to inspect or obtain a copy of PHI maintained in a designated record set. Such request may be required to be in writing. 30 days is the time deadline.
5. If the entity grants the request, it must provide the access requested
6. It must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format, or, in a readable hard copy form
7. The entity may provide a summary of the PHI requested if the individual agrees to the summary in advance, and to any fees imposed.
8. The entity must provide the access, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mailing the copy of the PHI at the individual's request
9. Fees: A reasonable cost-based fee may be imposed. (164.524 (c)(4)) The fee may only include the cost of:
 - a. Copying, including the cost of supplies and labor Postage
 - b. Preparing an explanation or summary of the PHI
10. If the entity denies the request for access to PHI, the entity must provide a timely, written denial to the individual. It must contain the basis for the denial, a statement of the individual's review rights, and a description of how the individual may complain to the entity or the Secretary.
11. If the entity does not maintain the PHI, but knows where the individual should request the information, the entity should direct the individual appropriately.

Amendment of Protected Health Information

1. An individual has the right to have an entity amend PHI or a record in a set, for as long as the PHI is maintained in the designated record set.
2. The entity may deny the request for amendment if it determines that:
 - a. The record was not created by the covered entity, unless the individual provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment
 - b. The record is not part of a designated record set
 - c. The record would not be available for inspection as noted in the regulation on access
 - d. The record is accurate and complete

3. The entity may require the amendment request be in writing and provide a reason to support an amendment. It must act within 60 days.
4. Mailing the amendment: After granting the request for amendment, the entity must:
 - a. Make the amendment by identifying the records affected by the amendment and linking them to the location of the amendment.
 - b. Inform the individual that the amendment is accepted and get the individual's agreement to have the covered entity notify the relevant persons identified by the individual.
 - c. Informing others in a reasonable time who need to know the amendment information.
5. Denying the amendment: If the entity denies the amendment, they must provide the individual a timely, 60 days or less, notice containing:
 - a. The basis for the denial
 - b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement. A statement that the individual may request that the entity provide the individual's request for amendment and the denial with any future disclosures.
 - c. A description of how the individual may complain to the covered entity
6. Statement of disagreement: The individual may submit a statement disagreeing with the denial. The entity may reasonably limit its length.
7. The entity may prepare a rebuttal statement and provide a copy to the individual.
8. The portions of the record must be identified and linked to the individual's statement of disagreement.
9. Future disclosures: The statement of disagreement with the request and denial for amendment must be included with subsequent disclosures, but it can be transmitted separately if not possible to be transmitted with the original documents.
10. Upon notice by another covered entity of amendment, the entity must amend the PHI.
11. The entity must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation.

Accounting of Disclosures of Protected Health Information (164.528)

1. An individual has the right to receive an accounting of disclosures of PHI made by the entity in the last six years, except for disclosures:
 - a. To carry out treatment, payment and health care operations
 - b. To individuals of PHI about them
 - c. For the facility's directory, or to persons involved in the individual's care
 - d. For national security or intelligence purposes
 - e. To correctional institutions or law enforcement official
 - f. That occurred prior to the compliance date for the covered entity

2. The accounting may be temporarily suspended at the request of a law enforcement agency during an investigation of the individual and an accounting would impede the activities of such agency. It can be limited for 30 days.

3. The accounting must be in writing, include the disclosures made in the last 6 years, as well as disclosures made by Business Associates, and must include the following:
 - a. The date of the disclosures
 - b. The name of the entity or person who received the PHI, and the address of such entity or person.
 - c. Brief description of the information disclosed.
 - d. Statement of purpose for basis of disclosure or, A copy of the individual's written authorization A copy of a written request for disclosure.
 - e. If multiple disclosures have been made, a summary of those disclosures may be provided.

4. The entity has 60 days to provide such an accounting.- It may extend the time by 30 days, if the individual receives a written statement of the reasons for the delay and the date by which the entity will provide the accounting.

5. The entity will provide the first accounting to an individual in any 12-month period without charge. The entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12 month period, provided the individual is informed of the fee, and has the opportunity to withdraw or modify the request.

6. The entity must document and retain:
 - a. The information required to be included in the accounting
 - b. The written accounting provided to the individual
 - c. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

MAKE A LIST OF THE PHI THAT IS RELEASED WITHOUT THE INDIVIDUAL'S CONSENT.

SECTION 4

THE PRIVACY RULES ORGANIZATIONAL REQUIREMENTS

THE PRIVACY RULES: ORGANIZATIONAL REQUIREMENTS

I. Use and Disclosure for Marketing

- A. The entity must have consent in order to use or disclose PHI for marketing purposes
- B. Exceptions: An entity may disclose PHI when making a marketing communication to an individual that:
 - 1. Occurs in a face to face encounter
 - 2. Concerns products or services of nominal value
 - 3. Concerns the health-related products and services of the covered entity or a third party and the communication
- C. The communication must:
 - 1. Identify the entity as the party making the communication
 - 2. State if the entity will receive remuneration for making communication
 - 3. Contain instructions describing how the individual may opt out of receiving such communication (except mass mailings)
- D. If entity uses PHI to target the communication to certain individuals:
 - 1. The entity must determine prior to the communication that the product will be beneficial to the health of those targeted
 - 2. The communication must explain why the individual was targeted

II. Uses and Disclosures for Fundraising

- A. Entity may disclose demographic information and the dates of service to a Business Associate for the purpose of raising funds for its own benefit.
- B. Entity must state in the Privacy Notice that it will be using PHI for fundraising purposes
- C. Include in any materials sent to an individual a description of how the individual can opt out of receiving such materials

III. Business Associates (BA) (164.502(e), 164.504(e))

- A. Definition: On behalf of such covered entity or of an organized health care arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of:
 - 1.) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
 - 2.) Any other function or activity regulated by this subchapter; or

3.) Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in Sec. 164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

B. Roles and Services

C. Entity may disclose PHI to a BA if there is satisfactory assurance the BA will safeguard the information.

D. When it does not apply

1. To a provider concerning treatment
2. To a health plan sponsor
3. Certain government programs

E. Contractual requirements

1. Establish permitted and required uses
2. Prohibit other uses
3. Require safeguards
4. Require BA to report unauthorized use
5. BA to provide access, amendments and accountings to individuals
6. Destruction or return of information
7. Termination of contract

F. Liability of entity with regard to BA

1. No duty to monitor (unless evidence of breach)
2. Non-compliance if entity knew BA had breaches

G. Procedures

1. Inventory all agreements and contracts
2. Identify those which apply to rule
3. Amend as necessary
4. Other

IV. Notice of Privacy Practices (164.520(a-c))

A. Right of Notice

1. Individual has the right to adequate notice of use and disclosure of PHI by the entity, and of the individual's rights and entity's legal duties
2. Exceptions:
 - a. Who in various group health plan relationships must provide the notice
 - b. Inmates in correctional institution

B. Content of Notice

1. Header:

“THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE READ IT CAREFULLY.”

2. Uses and Disclosures: Must contain:

- a. A description with at least one example of the types of uses and disclosures the entity is permitted to make
- b. A description of each of the other purposes for which the entity is permitted to use or disclose PHI without the individual's consent
- c. If disclosure above is prohibited or limited by other law, the description of such use must reflect the more stringent law
- d. The notice must have sufficient detail to place the individual on notice
- e. A statement that other uses and disclosures will be made only with the individual's authorization and that the individual may revoke the authorization

3. Separate statements for Certain Uses or Disclosures

- a. Appointment reminders, or treatment alternatives
- b. Fundraising
- c. A Health plan may disclose to the sponsor of the plan

4. Individual Rights: Must contain a statement of the individual's rights and a brief description of how they may exercise these rights

- a. Right to request restrictions on certain uses
- b. Right to receive confidential communications of PHI
- c. Right to inspect and copy PHI
- d. Right to amend PHI
- e. Right to receive an accounting of disclosures
- f. Right to receive a paper copy of the notice

5. Entity's Duties: The notice must contain:

- a. A statement that the entity is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI
- b. A statement that the entity is required to abide by the terms of the notice currently in effect
- c. A statement that the entity reserves the right to change the terms of its notice and to make the new notice effective for all PHI that it maintains

6. Complaints: The notice must contain:

- a. A statement that individuals may complain to the entity and the Secretary
- b. A description of how the individual may file a complaint,
- c. A statement that the individual will not be retaliated against

7. Contact: Who (name or title) and phone number to contact for further information

8. Effective Date

9. Revisions to the Notice: Must be made promptly whenever there is a material change

C. Provisions of Notice:

1. Health Plans
2. Entities with Direct Treatment Relationships
3. Electronic Notices

D. Joint Notices: Covered entities that participate in organized healthcare arrangements may comply with the notice requirements by a 'Joint notice"

V. The Privacy Officer and Duties (164.530(a))

The entity must designate a privacy official who is responsible for the development and implementation of the privacy policies and procedures of the entity.

A. Development of Policies

1. Review current policies and procedures for compliance with Rule
2. Decide who has and needs access to what PHI
3. Update, change, develop as necessary

B. Implementation of Policies

1. Training of staff in relevant policies and procedures
2. Evaluate effectiveness of training and implementation
3. Are there conflicts'?
4. Are there gaps between the policies and the Rule'?

VI. Training (164.530(b))

- A. A covered entity must train all members of its workforce:
 1. By the compliance date
 2. To each new member of its workforce
- B. The entity must document the training has been provided

VII. Safeguards (164.530(c))

- A. The entity must have the administrative, technical, and physical safeguards in place to protect the privacy of PHI.
- B. The entity must reasonably safeguard PHI from intentional or unintentional use or disclosure.

VIII. Complaints (164.530(d))

- A. The entity must provide a process for individuals to make complaints concerning the entity's policies and procedures
- B. The entity must document all complaints and disposition.

IX. Sanctions (164.530(e))

- A. The entity must have and apply sanctions against members of its workforce who fail to comply with privacy policies and procedures of the entity.
- B. Sanctions applied, if any, must be documented

SECTION 5

Organizational Tasks

(“A list of things to do” or “Where to get started”)

1. Buy or download the HIPAA regulations from the Federal Register. You can access it on-line at the HCFA's Web Site at <http://www.hcfa.gov> , or at <http://aspe.hhs.gov/admsimp/Index.htm>.
2. Gather other resources for practical use;
<http://www.aha.org> : American Health Information Management Association. Great source for briefs on a variety of topics addressed by HIPAA, and you don't have to be a member to access.
<http://www.aha.org> : American Hospital Association. Must be a member to have access to most of the resources.
<http://www.himss.org> : Healthcare Information and Management Systems Society
<http://www.jhita.org> : Joint Healthcare Information Technology Alliance
3. Formalize the planning process. Request resources to plan and implement the regulations. Think about a Privacy Committee to maximize internal experts.
4. Read the rules. Don't skip this step.
5. Appoint the Privacy Officer. Determine the duties of the Privacy Officer. (Look at the AHJMA web site for a sample job description)
6. Establish an oversight board for research projects if your facility does not have one (such as an IRB).
7. Review all policies regarding patient information and privacy. Include the entire organization, not just the Health Information (Medical Record) Department.
 - a. Review classes of employees against the information they need to perform their work. Determine who has access to what.
 - b. Decide how the "minimum necessary" will be determined and who will make that decision. Then determine "minimum necessary" for each job class.
 - c. Review all consents, notices of information practices, authorization forms, and compare with the HIPAA requirements.
 - d. Review the existing policies for patients obtaining and amending their records
 - e. Review the Washington State laws regarding privacy to determine the more stringent applications.
 - f. Review all policies regarding directories, marketing, fund raising, d~ identification
8. Formalize the information sent on a routine basis, when written authorization is not required:

- a. Disclosures for treatment, payment, and health care operations
- b. Disclosures to business associates
- c. Disclosures to public health authorities
- d. For health oversight activities
- e. For coroners and medical examiners
- f. For directory information
- g. For research purposes
- h. For emergency situations

9. Evaluate and determine training needs for ALL facility employees, volunteers, medical and professional staff, business associates, etc.

Determine training needs of all classes of employees job specific) Determine which volunteers, business associates, etc. need training

10. Review all "contractual" employees. Determine if they qualify as business associates, and need a formal contract or agreement.

10. Review all business associate contracts for applicability to the Rule, and for those needing to be amended~ Determine approach with those who will not want to amend contract.

- a. Survey Business Associates to determine what information they see
- b. Review contracts to ensure privacy requirements are included
- c. Review contracts to address return/destruction of information
- d. Review contracts to address non-compliance with privacy
- e. Review contracts to address individual inspection/amendment
- f. Inventory all agreements

11. Develop tracking/accountability methods with Business Associates to ensure the privacy of health information in their control

12. Develop policies, if needed, for giving an accounting of access of PHI in order to give to individuals who request one.

13. Determine need for complaint process re: Privacy. Remember complaints can be lodged with the Secretary or with Civil Rights. Determine organizational authority to receive and resolve.

14. Develop a written statement to be signed by all employees upon employment. Develop sanctions policies for failure to comply with the privacy policies for all individuals in the work force and for all business associates. Develop an annual review policy.

15. Compare the security rules with those currently in effect.