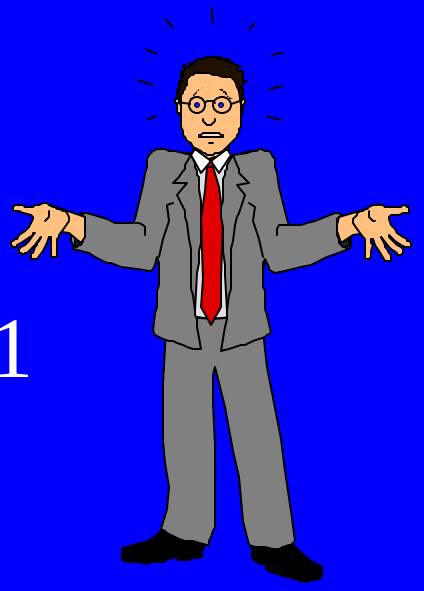
HHS Guidance for Privacy Under HIPAA

Guidance Issued July 6, 2001



Privacy Rule

- Gives patients more control over Patient Health Information (PHI)
- Sets boundaries on the use and release of PHI
- Establishes safeguards
- Holds violators accountable with civil and criminal fines and penalties

Privacy Rule (cont.....)

- Enables patients to find out how their PHI may be used and what disclosures have been made
- Limits the release of information to the "minimum reasonably needed" for the purpose of disclosure
- Gives patients the right to examine and obtain a copy of their PHI and request changes

General Provider Privacy Requirements

- Provide patients info on rights
- Adopt clear privacy procedures
- Train all individuals under the institution's control
- Designate a person to manage implementation
- Secure PHI so it is not readily available to those who do not need access

Scope of Privacy Rule--Covered Entities

- Health Plans
- Health Care Clearinghouses
- Health care providers who conduct certain financial and administrative transactions electronically
- Business Associates of Covered Entities

Compliance Date

- Providers, large Health Plans, Clearinghouses--April 14, 2003
- Small Health Plans--April 14, 2004

- The HHS Office of Civil Rights (OCR) will assist with compliance--http://www.hhs.gov/ocr/hipaa/.

Areas of Potential Change in Rule Per Sec. Thompson

- Phoned-In Prescriptions
- Referral Appointments-no need for patient consent to make initial appointments
- Allowable Communications-entities are still free to engage in any necessary discussions for effective high quality health care
- Minimum Necessary Scope-sign-in sheets, x-ray lightboards, charts at bedside are NOT prohibited under Privacy Rule

Consents

- A written consent is required before using or disclosing a patient's PHI to carry out treatment, payment, or health care operations (TPO)
- Exception:No consent is necessary in an emergency, when a provider is required by law to treat the patient, or when there are substantial communication barriers

Consents (cont.....)

- Providers having indirect treatment relationships with patients (e.g.. Laboratory, Health Plans, and Clearinghouses) may use PHI and disclose PHI without consent--they may obtain consent if they choose
- If a patient refuses to consent to the disclosure of PHI for TPO, a provider may refuse treatment
- A written consent for TPO is only required once

Consent (cont.....)

- The consent document may be brief and written in general terms
- A consent must: be written in plain language, inform the individual that PHI may be used for TPO, state the patient's rights to review the Privacy Notice, to request restrictions and to revoke consent, and must be signed and dated by patient or patient's legal representative

Consent-Individual Rights

- A patient may revoke consent in writing, except if the provider has acted in reliance on the consent
- A patient may request restrictions on the use and disclosure of PHI-the provider may disagree with the restriction
- A patient must be given notice of the Covered Entity's privacy practices and may review notice prior to consent

Consent-Administrative Issues

- Consents must be retained for 6 years from date last in effect--for our patient population, we may need to keep longer
- Integrated Covered Entities may obtain on joint consent for multiple entities and sites
- If a Covered Entity receives consent, only the Minimum Necessary PHI may be disclosed

Consents vs. Authorizations

- Consent: general document that gives providers permission to use and disclose PHI for TPO-one consent may cover all uses and disclosures for TPO by that provider indefinitely
- Authorization: more customized document that gives covered entities permission to use specified PHI for specified purposes-other than TPO-and it has an expiration date

Special Authorization Req....

- Providers must obtain an authorization- NOT a Consent, to use or disclose PHI maintained in psychotherapy notes for treatment by persons other than the originator of the notes, for payment, or for health care operations

Minimum Necessary Rules

- General Rule: Providers must take reasonable steps to limit the use and disclosure of PHI to the minimum necessary to accomplish the intended purpose
- Exceptions: disclosures for TPO, disclosures to patient, disclosures that are authorized, disclosures req.. for HIPAA transactions, disclosures req.. by law

Minimum Necessary Rules

- Policies and Procedures must be developed to identify persons or classes of persons who need access to PHI, the categories of PHI needed, and conditions appropriate to such access
- Hospitals may implement policies that permit doctors, nurses, or others involved in treatment to access the entire medical record-a justification must be included in the policy
- For non-routine disclosures, providers must have criteria for determining and limiting access to PHI

Minimum Necessary Rule

- Reasonable Reliance: a Covered Entity may rely on the judgment of the party requesting the disclosure as to the minimum PHI needed
- Reliance is permitted when request made by: public official, another Covered Entity, Professional who works with the Covered Entity or Business Associate
- A PI with documentation from IRB or Privacy Board

Minimum Necessary Rules

- Minimum Necessary includes residents, medical students, fellows, nursing students access to PHI for TPO
- Disclosures for treatment purposes between health care providers are exempted from the minimum necessary requirements
- Sign in sheets are NOT prohibited and guidance is forthcoming from HHS

Oral Communications

- HHS will publish guidance on oral communications, which are covered under the Privacy Rule
- Covered Entities must make reasonable efforts to prevent uses and disclosures of PHI not permitted by law--policies and procedures are necessary
- Suggestions: speaking quietly in patient areas, avoiding using patient names in hallways and elevators, having curtains or cubicles for registration, etc.

Business Associates

- Business Associates: persons or entities who provide functions, activities, or services for or to a covered entity, involving the use or disclosure of PHI-physicians with admitting privileges to a hospital are not business associates and no separate agreement is required

Business Associates

- A provider may only disclose PHI to a Business Associate by obtaining a contract with satisfactory assurances that the Business Associate will use the information only for the purposes for which they were engaged, will safeguard the information from misuse, and will help the Covered Entity comply with providing patients an accounting of disclosures of PHI

Parents and Minors

- A parent is generally a “personal representative” of a minor child and as such, may access PHI unless such disclosure would otherwise not be allowed under state law
- If a minor can consent to treatment under state law, a parent may not obtain the minor’s PHI unless he/she is authorized by the minor child

Health-Related Marketing

- Marketing: a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service
- What is NOT Marketing:describing providers in a plan or network, communications that are part of treatment (e.g.. Brand name drugs vs. generic), communications made to further treatment (e.g.. Notices of future appointments, etc.)

Limitations on Marketing

- If a communication is marketing, a Covered Entity may use or disclose PHI to create or make the communication only if:
  - it is a face to face communication
  - it involves products or services of nominal value
  - it identifies the Covered Entity making the communication, states that the Covered Entity is being paid for making the communication, tells patients how to avoid future marketing, explains why specific patients were targeted--all other marketing requires patient's authorization!!

Research

- The Privacy Rule defines the means by which human research subjects are informed of how their medical information will be used or disclosed and their rights with regard to gaining access to information, when such information is held by Covered Entities

Research (cont.....)

- Covered Entities are permitted to use and disclose PHI for research with individual authorization, or without individual authorization, under limited circumstances under the Privacy Rule

Research (cont.....)

- To use or disclose PHI WITHOUT individual authorization, a Covered Entity must obtain one of the following:
  - Documentation that a waiver of authorization has been approved by the IRB or a Privacy Board
  - Representations from the PI, either in writing or orally, that the use or disclosure of the PHI is solely to prepare a research protocol, that the PI will not remove any PHI from the Covered Entity, and the representation that PHI for which access is sought is necessary for the research
  - Representations from the PI, in writing or orally, that the use or disclosure is solely for research on PHI of decedents, that the PHI being sought is necessary for the research, and documentation of the death of the subject

Research (cont.....)

- A Covered Entity may use or disclose PHI for research purposes with a waiver of authorization by an IRB or Privacy Board if it has ALL of the following documentation:
  - A statement that the waiver was approved by the IRB or Privacy Board
  - A statement identifying the IRB or Privacy Board and the date on which the waiver was approved, and….

Research (cont.....)

- A statement that the IRB or Privacy Board has determined that the waiver of authorization, in whole or in part, satisfies 8 criteria:
  - Use or disclosure poses minimal risk to patient
  - Waiver will not affect privacy rights
  - Research could not be done without waiver
  - Research could not be done without PHI
  - Risks are reasonable compared to benefits
  - Plan to protect the identifiers from improper use and disclosure
  - Plan to destroy identifiers at appropriate time
  - Assurances that PHI will not be reused

Research (cont.....)

- Additional documentation requirements to use PHI per a waiver of authorization:
  - A brief description of the PHI for which use or access is necessary by the IRB or Privacy Board
  - A statement that the waiver has been approved under either normal or expedited review procedures
  - The signature of the chair or other member, of the IRB or Privacy Board

Research (cont.....)

- Use/Disclosure WITH individual authorization-authorizations should include:
  - any elements of the research protocol to be reimbursed under the subject's health plan

Research (cont.....)

- Other considerations:
  - For multi-site research research that requires PHI from two or more covered entities, Covered Entities may accept documentation of IRB or Privacy Board approval from a single IRB or Privacy Board
  - A Covered Entity may use PHI to create a research database so long as there is documentation that the IRB or Privacy Board has determined that waiver criteria are met

Research (cont.....)

- Other considerations:
  - For minimal risk research, IRBs and Privacy Boards can use an expedited review process permitting documentation of approval of only one or more members of the IRB or Privacy Board

Conclusion

- The HHS Office of Civil Rights has been assigned responsibility to enforce the Privacy Rule
- HIPAA compliance and enforcement is on HHS's priority list--the time to plan is NOW