HIPAA

Administrative Simplification: Privacy, Security, and Compliance

William R. Braithwaite, MD, PhD
"Doctor HIPAA"

NCHCC
Washington, DC

February 6, 2003

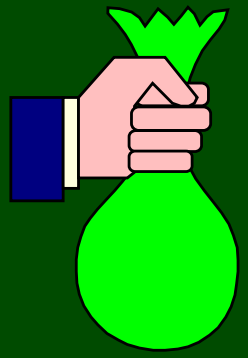
PRICEWATERHOUSECOOPERS

1996: HIPAA Passes

Administrative Simplification Tags Along

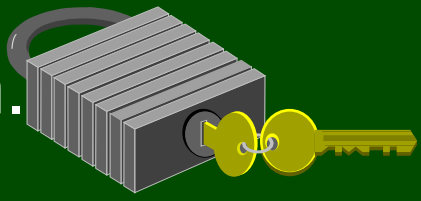
Administrative Simplification Reality

- Save money by setting standards and requirements for electronic transmissions.



- AND

- Protect security and privacy of individually identifiable health information.

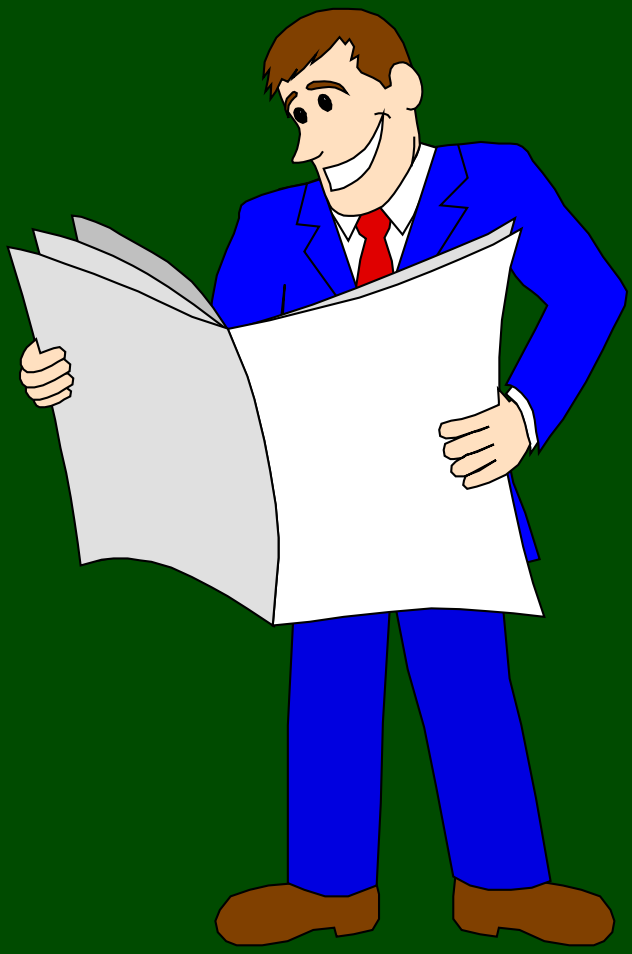


It's a package deal!

The deep water of federal regulations …

Federal Register Publications

- Privacy NPRM - 11/3/99
  - Final Rule - 12/28/00
  - Guidance issued 7/6/01
  - Modifications NPRM 3/27/02
  - Final Rule with Modifications 8/14/02
  - More guidance issued 12/3/02
  - Compliance by 4/14/03
- Security NPRM - 8/12/98
  - Final Rule expected 2/28/03
  - Compliance by 4/28/05



I just want to be let alone!

Definitions for Privacy

Privacy is the right of an individual to

- control personal information and
- not have it disclosed or used by others without permission.

Confidentiality is the obligation of another party to respect privacy by

- protecting personal information they receive and
- preventing it from being used or disclosed without the subject's knowledge and permission.

Security is the means used protect the integrity, availability and confidentiality of information.

- physical, technical and administrative safeguards

Principles of Fair Info Practices

Notice

- Existence and purpose of record-keeping systems must known.

Choice – information is:

- Collected only with knowledge and permission of subject.
- Used only in ways relevant to the purpose for which the data was collected.
- Disclosed only with permission or overriding legal authority.

Access

- Individual right to see records and assure quality of information.
  - accurate, complete, and timely.

Security

- Reasonable safeguards for confidentiality, integrity, and availability of information.

Enforcement

- Violations result in reasonable penalties and mitigation.

Bare Bones of HIPAA Privacy Standards

Scope: What is Covered?

Protected health information (PHI) is:

- Individually identifiable health information,
- Transmitted or maintained in any form or medium,
- Held by covered entities or their business associates.

De-identified information is not covered.

- Specific rules determine de-identification.

Designated Record Set

A group of items of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

Individual's Rights

Individuals have the right to:

- A written notice of information practices from health plans and providers.
- Inspect and obtain a copy of their PHI (DRS).
- Obtain an accounting of disclosures.
- Amend their records.
- Request restrictions on uses and disclosures.
- Accommodation of reasonable communication requests.
- Complain to the covered entity and to HHS.

Key Points

Covered entities can provide greater protections if they want.

Required disclosures are limited to:

- Disclosures to the individual who is the subject of information.
- Disclosures to OCR to determine compliance.

All other uses and disclosures in the Rule are permissive.

Uses and Disclosures

Must be limited to only what is permitted under 4 mechanisms in the Rule:

- Treatment, payment, and health care operations (TPO) after notice and acknowledgement.
- Uses and disclosures involving the individual's care or directory assistance,
  - Requiring an opportunity to agree or object.
- For specific public policy exceptions.
- All others as authorized by individual.

Requirements vary based on type of use or disclosure.

Health Care Operations examples

- outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies.
- population-based activities relating to:
  - improving health or reducing health care costs,
  - protocol development,
  - case management and care coordination,
  - contacting of health care providers and patients with information about treatment alternatives.
- evaluating performance of providers and plans.
- training programs.
- accreditation, certification, licensing, or credentialing.

Consent, Notice, and Acknowledgement

"Consent" or permission to use PHI for TPO is assumed when you go to a health care provider.

- CE may obtain written consent, if they wish.

Direct treatment provider must provide Notice of Privacy Practices as soon as reasonably practicable and then make a good faith effort to obtain a written acknowledgment of receipt.

- If not obtained, document good faith efforts to obtain acknowledgment and the reason why the acknowledgment was not obtained.

Acknowledgement is not required for:

- Indirect Treatment Providers,
- Health Plans,
- Health Care Clearinghouses.

Policy Exceptions

Covered entities may use or disclose PHI without a consent or authorization only if the use or disclosure comes within one of the listed exceptions & certain conditions are met;

- As required by law.
- For public health.
- For law enforcement.
- Coroners, medical examiners, funeral directors.
- …
- Health care oversight.
- For research.
- Organ transplants.

Authorizations (not TPO)

Generally, covered entities must obtain an individual's authorization before using or disclosing PHI for purposes other than treatment, payment, or health care operations.

- Most uses or disclosures of psychotherapy notes also require authorization.

Provider marketing and fundraising may require authorization.

How much information is enough?

Minimum Necessary

Covered entities must make reasonable efforts to limit the use or disclosure of PHI to minimum amount necessary to accomplish their purpose.

Exceptions:

- Disclosure to or request by provider for treatment.
- Disclosure to individual.
- Under authorization (unless requested by CE).
- Required for HIPAA standard transaction.
- Required for enforcement.
- Required by law.

Minimum Necessary: Rule

Reasonableness standard -

- consistent with best practices in use today.

"Role-based" access limits.

Standard protocols for routine & recurring uses and disclosures.

Criteria for review of each non-routine disclosure.

May rely on judgment of requestor if:

- public official for permitted disclosure.
- covered entity.
- professional within covered entity.
- BA for provision of professional service for CE.
- researcher with IRB documentation.

Oral Communication

All forms of communication covered.

Requires reasonable efforts to prevent impermissible uses and disclosures.

- Given such efforts, incidental disclosures are not violations.

Policies and procedures to limit access/use

- except disclosure to or request by provider for treatment purpose.

Using PHI for Research Purposes

6+ ways PHI can be used for research:

1. De-identified PHI
2. Limited Data Set with Data Use Agreement
3. PHI with IRB/Privacy Board waiver
4. PHI for research protocol preparation
5. PHI of deceased
6. PHI with authorization of subject

plus, Healthcare Operations, Public Health, and as otherwise required by law (registry, reportable).

How does HIPAA affect research?

- New burdens for IRBs.
- Voluntary registries must now get patient authorization.
- Liability fears may dissuade providers from sharing data with researchers.
- New forms for research subjects.
- Health Plans and Providers must track and account for research disclosures made without authorizations.

Special Rules for Group Health Plans

- Generally, the plan sponsor may only receive information from the group health plan or its vendors to carry out "plan administration functions" if it:
  - 1) modifies its plan documents,
  - 2) places the proper controls on the flow of PHI, and
  - 3) issues a certification to the group health plan about the protections applied to the information.
- "Plan administration functions" do not include employment–related functions or functions related to other plans.
- Amendments and certifications must:
  - Establish uses and disclosures of PHI by the plan sponsor and its agents, and
  - Ensure adequate separation between group health plan and plan sponsor.
    - Accurate job descriptions
    - Policies and procedures to enforce separation
    - Recusal from employment decisions
- If no changes in plan documents and practices or no certification:
  - Sponsor may only receive "summary" information from its vendors, and
  - only in the contexts of premium bids and of modifying, amending or terminating the plan.

Rule #1: Don’t surprise the patient!!!

Impact of HIPAA Privacy Standards

HIPAA preempts or supercedes all "contrary" state laws.

- Exceptions:
  - HHS determination that State law accomplishes social responsibilities (fraud & abuse, industry oversight, health & safety).
  - Public health reporting.
  - State privacy law that has:
    - More restrictive use/disclosure rules.
    - Greater rights for individuals.
- Result: different privacy environment in each state.
  - No ERISA preemption

May Exacerbate Liability

- HIPAA raises industry's "standard of care" in tort claims.
- HIPAA increases awareness, media coverage and enforcement of a complex patchwork of laws, rules, and standards.
  - forces everyone to get control of their channels through which individual health information flows.

Other Privacy Drivers

E.U Data Directive

E.U – U.S. Safe Harbor

New federal privacy law being proposed

State Privacy Laws (new state laws)

Consumer Protection Law (State)

Federal Trade Commission (Eli Lilly).

Internet Privacy (e.g., COPPA)

Reputation Assurance

Business Disruption prevention

The Future of HIPAA

Future of Privacy

States are passing privacy law that is more stringent than HIPAA and/or covering more entities.

Federal law may follow suit after consensus of states pass similar laws.

Organizations taking long view are likely to implement broad privacy program based on 5 principles of fair information practices,

- rather than minimal compliance approach.

Security Requirements in Privacy

Implementation specification: safeguards.

- "A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart."

Specific Security in Privacy

Role-based access required under minimum necessary rule.

Verification and authentication of individuals and authorities requesting PHI.

Security required by Privacy Rule applies to protected health information in all forms.

- Security Rule only applies to electronic info.

Security Requirements in HIPAA

Covered Entities shall maintain reasonable and appropriate administrative, technical, and physical safeguards --

- to ensure integrity and confidentiality
- to protect against reasonably anticipated
  - threats or hazards to security or integrity
  - unauthorized uses or disclosures
- taking into account
  - technical capabilities
  - costs, training, value of audit trails
  - needs of small and rural providers

Key Security Philosophy

Identify & assess risks/threats to electronic info:

- Availability
- Integrity
- Confidentiality

Take reasonable steps to reduce risk.

Involves policies/procedures & contracts with business associates more than technology.

- For security technology to work, behavioral safeguards must also be established and enforced.
  - requires administration commitment and responsibility.

BE REASONABLE!

Expected Security Final Rule

Definitions and applicability harmonized with privacy.

Requirements clarified and redundancies removed.

Same philosophy as NPRM.

- Organization specific risk analysis and documentation of decisions.
- Only applies to electronically maintained and transmitted health information.
- Continues to be technology neutral.

No electronic signature standard.

General Security Rule Structure

Rule composed of standards, each of which may have required and addressable implementation specifications.

CE must assess, and document, whether each addressable implementation specification is a reasonable and appropriate safeguard in its environment, … taking into account the following factors:

Assessment Factors

- The technical capabilities of record systems used to maintain electronic protected health information;
- The costs of security measures;
- The need for training persons who have access to electronic protected health information;
- The value of audit trails in computerized record systems; and
- The size, complexity, and capabilities of the covered entity, and
- Implement the specification where reasonable and appropriate;
  or document the rationale behind a decision to implement alternative measure(s) to meet the standard.

Administrative Requirements

Apply to both privacy and security.

Flexible & scalable (i.e., requires thought!).

Covered entities required to:

- Designate a responsible official (privacy/security).
- Develop policies and procedures (including on receiving complaints).
- Provide training to its workforce.
- Develop a system of sanctions for employees who violate the entity's policies.
- Meet documentation requirements.

Business Associates

<u>Only</u> covered entities are subject to the rules.

- this limit doesn't make sense
  - because healthcare uses outsourcing extensively and
  - these other entities would not be required by law to safeguard our health information …

- … so 'business associate agreements' were invented to obligate outsource agents, vendors, and contractors to safeguard the health information they need to do their jobs.

Business Associates

Agents, contractors, others hired to do work of or for covered entity that requires PHI must provide Satisfactory Assurance:

- An agreement – usually a contract – that a business associate will safeguard the protected health information.

No business associate relationship is required for disclosures to a health care provider for treatment.

Business Associates (2)

Covered entity is responsible for actions of business associates, if:

- knew of violation of business associate agreement
- failed to act.

Liability only when:

- CE is aware of material breach &
- fails to take reasonable steps to cure breach or end relationship.

Monitoring is not required.

Complex Organizational Arrangements

University is likely a hybrid entity,

- with some separable health components.

Hospital is likely separate legal entity;

- may be part of affiliated entity (hospital chain).

MD Practice Plan is likely covered entity,

- with many Business Associates and
- complex relationships within the healthcare community.
- may benefit from Affiliated Entity or Organized Health Care Arrangement status.

'Entity Analysis' required to sort out needs and requirements for large, complex entities.

HIPAA Enforcement: Watching, Listening

Enforcement by HHS

Enforcement by investigating complaints.

- not HIPAA police force -- OCR not OIG for privacy.

Fines by HHS are unlikely (and small).

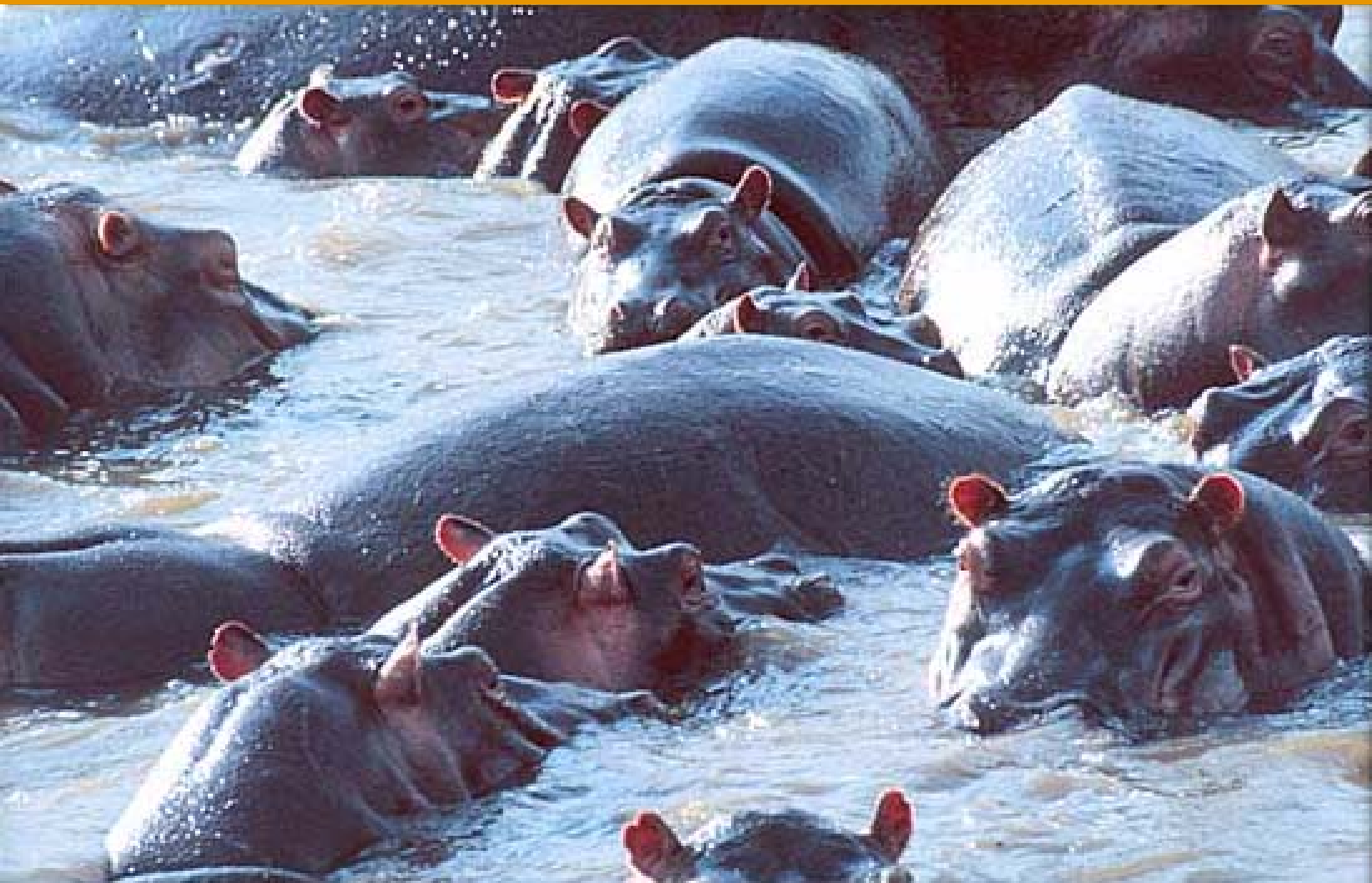
Fines and jail time possible from DOJ.

- Where intent can be proven.

BUT, real risk comes from

- Civil liability from private lawsuits.
- Federal Trade Commission (Eli Lilly).
- New privacy laws (federal and state).

Working Together to Get the Job Done



Questions?

William.R.Braithwaite@us.PwCglobal.com

http://www.pwchealth.com/hipaa.html

http://aspe.hhs.gov/admnsimp

http://www.hhs.gov/ocr/hipaa

www.cms.hhs.gov/hipaa/

ncvhs.hhs.gov

www.wedi.org

snip.wedi.org

Only 67 days left!