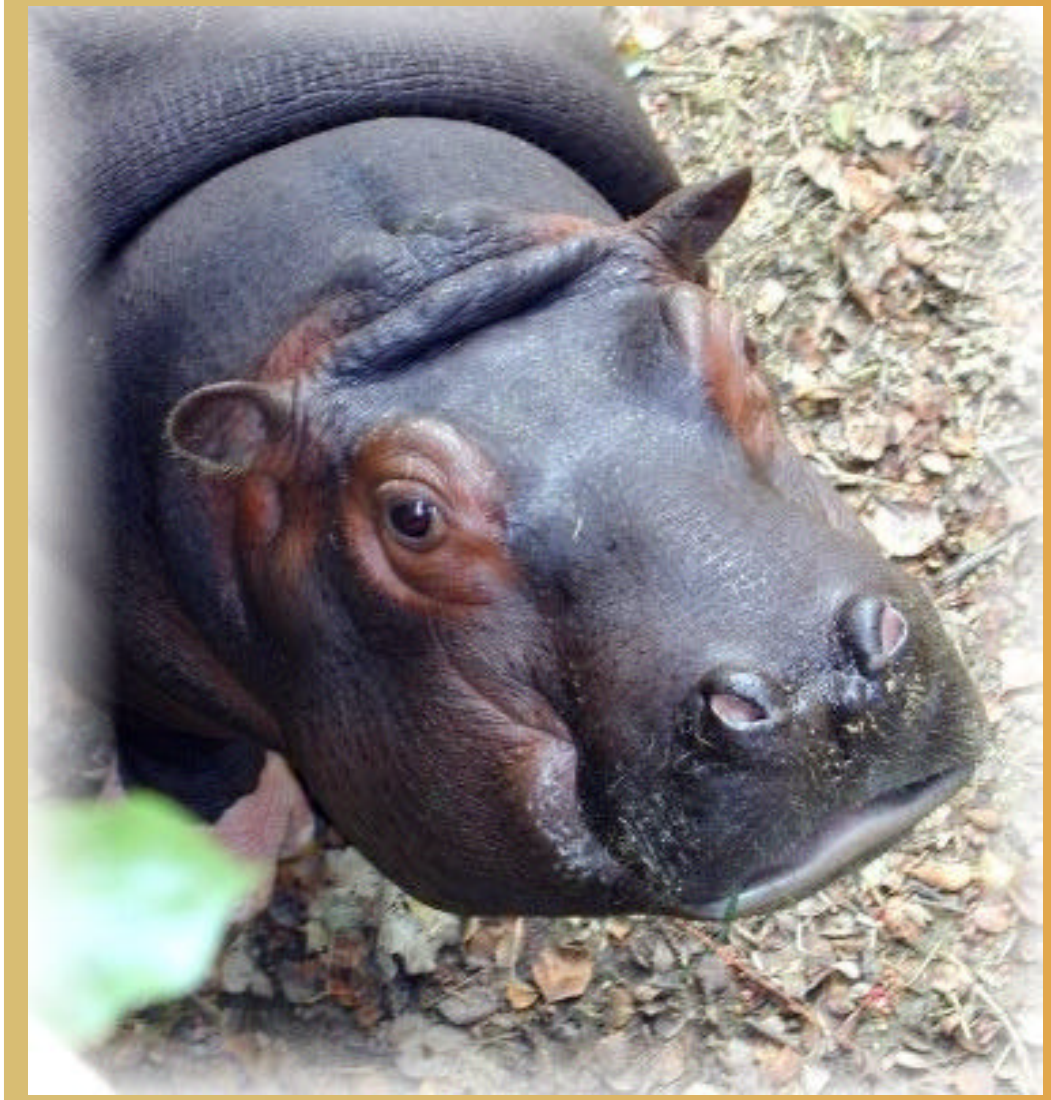
# HIPAA Administrative Simplification



## Health Information Privacy

*William R. Braithwaite, MD, PhD*

*"Dr. HIPAA"*

HIPAA Summit West II
San Francisco, CA
*March 14, 2002*

PRICEWATERHOUSECOOPERS

# Requirements for Privacy

**HIPAA requires:**

- "Standards with respect to the privacy of individually identifiable health information …"

- Final Rule published 12/28/2000
- Guidance issued 7/6/01.
- Compliance required 4/14/2003.

- Modifications will be proposed in NPRM soon.
  - Expect proposals to decrease administrative burden.
  - Expect no change in compliance date.

# 5 Principles of Fair Info Practices

**Openness [Notice]**

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

**Individual Participation [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.

**Accountability [Enforcement]**

- Violations result in reasonable penalties and mitigation.

**Limits on Collection, Use, and Disclosure [Choice]**

- Information collected only with knowledge and consent of subject.
- Information used only in ways relevant to the purpose for which the data was collected.
- Information disclosed only with consent or legal authority.

# 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.**

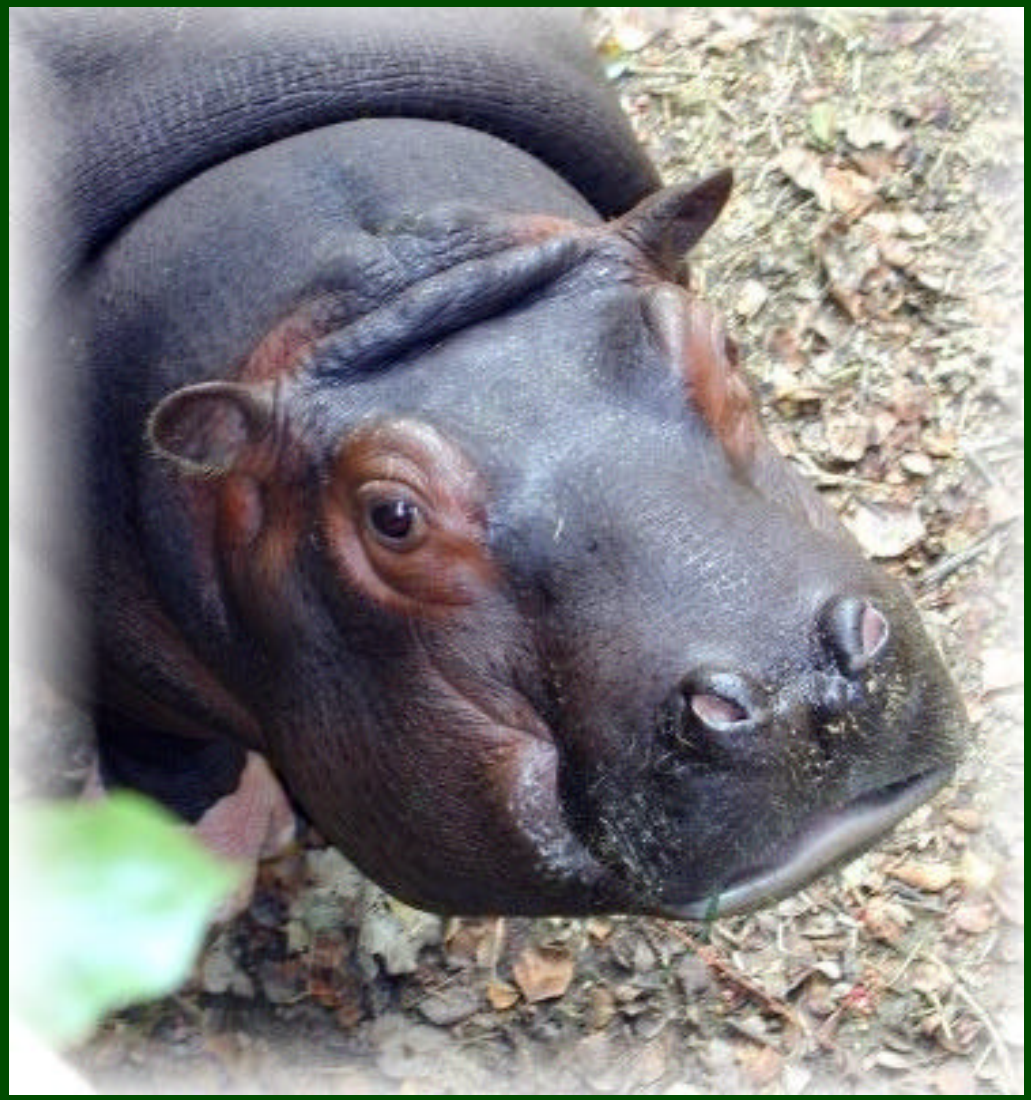
- Specific rules determine de-identification.

# 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.
- 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.

# I just want to be left alone!



PricewaterhouseCoopers

# 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 what is permitted in the Rule:**

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

**Requirements vary based on type of use or disclosure.**

# Consent: Rule

**Written consent required before direct treatment provider may use PHI for TPO.**

**Exceptions:**

- emergency treatment situation,
- substantial communication barriers,
- when required by law to treat.

**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.
- Health care oversight.
- For public health.

# Policy exceptions, (2)

- For research.
- For law enforcement.
- For judicial proceedings.
- For other specialized government functions.
- To facilitate organ transplants.
- To Coroners, medical examiners, funeral directors.

# 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 require authorization.**

# HIPAA: it not only looks complicated …

# 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 / disclosures.**

**Review 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.**

**Policies and procedures to limit access/use**

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

# Business Associates

**Agents, contractors, others hired to do work of or for covered entity that requires PHI.**

**Satisfactory assurance – 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.**

# Administrative Requirements

**Flexible & scalable.**

**Covered entities required to:**

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

# Hippocratic Philosophy of Rule-Making

**First, do no harm …**

- to the patient
- to the provider
- to the parts of the system that work!

**Don't go too far …**

- either way
- reaction could kill it.

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

# Resources

**Office for Civil Rights Web Site:**

- http://www.hhs.gov/ocr/hipaa/
- for privacy related publications and questions.

William.R.Braithwaite@us.PwCglobal.com

P w c

Your worlds Our people