

# Privacy & Security Regulation

## National Congress on Health Care Compliance

William R. Braithwaite, MD, PhD  
Director, Healthcare Consulting Practice  
Washington, DC

7 February 2002, Washington, DC

P W C

# Contents

**International Fair Information Practices**

**HIPAA Privacy Requirements**

Scope

Uses and Disclosures

Consent vs. Authorization

Minimum Necessary Rule

State law & Preemption

**HIPAA Security Requirements**

**How to get more information**

# Fair Information Practices

## **“Records, Computers, and the Rights of Citizens” report by HEW Advisory Committee in 1973**

- led to Privacy Act of 1974 governing personal data held by US federal government.

## **OECD Guidelines and COE Conventions in 1981**

- fed into bills that failed in US Congress.

## **“Computer-based Patient Record” report by IOM in 1991 and WEDI reports in 1991 and 1993**

- led to Administrative Simplification Bill in 1994
  - adopts EDI, security, and privacy standards.
  - Passed as part of HIPAA in 1996.

# 5 Principles of Fair Info Practices

## **Openness**

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

## **Individual Participation**

- 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**

- Violations result in reasonable penalties and mitigation.

## **Limits on Collection, Use, and Disclosure**

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

# Requirements for Privacy

## **HIPAA requires:**

- Recommendations to Congress for legislation from the Secretary of Health and Human Services (done 9/97).
- If legislation establishing privacy standards is not enacted within 3 years, the Secretary of HHS shall promulgate final regulations containing such standards.

## **Final Rule published 12/28/2000**

- Guidance issued 7/6/01.
- Compliance required 4/14/2003.
- Administrative Simplification Compliance Act (AKA 'Delay' legislation)
  - does not affect privacy scope or compliance date.
- Modifications expected to be proposed early 2002.
  - Expect proposals to decrease administrative burden.
  - No change expected in compliance date.

# Scope: Who is Covered?

## **Limited by HIPAA to covered entities:**

- Health care providers who transmit health information in electronic transactions.
- Health plans.
- Health care clearinghouses.

## **Business associate relationships ...**

- Agents and contractors (not otherwise covered) who need health information to do work on behalf of covered entities.
- Covered entities required to contract for protection of the information.

# Scope: What is Covered?

## **Protected health information (PHI) is:**

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

## **De-identified information is not covered.**

- Specific rules determine de-identification.

# Uses and Disclosures

## **Limit to what is permitted in the Rule (4 conditions):**

- Treatment, payment, and health care operations (TPO).
  - Under conditions of notice and consent for direct providers.
- Uses and disclosures involving the individual's care or directory assistance,
  - Require an opportunity to agree or object.
- For specific public purposes.
  - Following controls and limits in rule.
- All others as permitted by individual.
  - Under written, revocable authorization.

**Specific requirements vary based on type of use or disclosure.**

# Consent

**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 certain conditions are met & the use or disclosure comes within one of the exceptions;**

- As required by law.
- For health care oversight.
- For public health.
- For research.
- To facilitate organ transplants.
- For law enforcement.
- For judicial proceedings.
- For other specialized government functions.
- To Coroners, medical examiners, funeral directors.

# 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 (2)

## **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.

# State Law & Preemption

## **State Health Information Privacy Laws are:**

- Fragmented, not comprehensive
- Scattered in all parts of state law
- Entity specific (e.g. aimed at a specific type of healthcare entity)
- Not uniform or kept up-to-date

## **HIPAA Administrative Simplification preempts most ‘contrary’ provisions of state law,**

- **Except** more stringent provisions of state law regarding privacy.

**Result: Each type of entity must perform (or have performed on its behalf) a legal analysis of the law in each applicable state with respect to HIPAA privacy rules to determine true requirements.**

- HHS not expected (or equipped) to do this.

# HIPAA Security Requirements

**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

**Proposed rule published August 12, 1998.**

**Final rule expected soon.**

# Key Security Philosophy

## **Identify & assess risks/threats to:**

- Availability
- Integrity
- Confidentiality

**Take reasonable steps to reduce risk.**

# Security Issues

**Covers data at rest as well as transmitted data.**

**Involves policies/procedures & contracts with business associates.**

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

**Final rule expected soon:**

- Harmonized with privacy (scope, philosophy).
- General requirements only (flexible, scalable, technology neutral).

**Electronic signatures:**

- Final rule will depend on industry progress on reaching consensus on a standard.

# For More Information

**OCR Privacy Website:**

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

**Administrative Simplification Web Site:**

<http://aspe.hhs.gov/admsimp/>

**Georgetown Health Privacy Project**

[www.healthprivacy.org](http://www.healthprivacy.org)

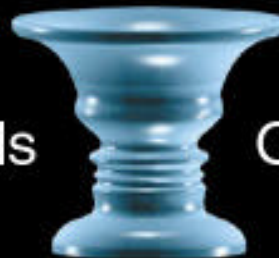
**William.R.Braithwaite@us.pwcglobal.com**

P

W

C

Your worlds



Our people