HIPAA

Administrative Simplification: Strategic Thinking in Compliance

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

National HIPAA Summit V
Baltimore, MD
October 31, 2002

Purpose of Administrative Simplification

“To improve the efficiency and effectiveness of the health care system

- by encouraging the development of a health information system

- through the establishment of standards and requirements for the electronic transmission of certain health information.”

HHS Required to Adopt Standards:

Electronic transmission of specific administrativ and financial transactions (including data elements and code sets)

- List includes claim, remittance advice, claim status, referral certification, enrollment, claim attachment, etc.
- Others as adopted by HHS.

Unique identifiers (including allowed uses)

- Health care providers, plans, employers, & individuals.
- For use in the health care system.

Security and electronic signatures

- Safeguards to protect health information.

Privacy

- For individually identifiable health information

Philosophically Speaking …

HIPAA Standards Philosophy

To save money:

- every payer must conduct standard transactions.
- no difference based on where transaction is sent.

Standards must be

- industry consensus based (whenever possible).
- national, scalable, flexible, and technology neutral.

Implementation costs must be less than savings.

Continuous process of rule refinement:

- Annual update maximum (for each standard) to save on maintenance and transitions.

Identifiers

Identifiers should contain no ‘intelligence’.

- Characteristics of entities are contained in databases, not imbedded in construction of identifier.

Identifiers should be all numeric.

- For easy telephone and numeric keypad data entry

Identifiers should incorporate an ANSI standard check digit to improve accuracy.

- Exception for Employer Identification Number [EIN]
  - Already exists and supported.

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 [Safeguards]

- 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]

- 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.

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

Key Security Philosophy

Identify & assess risks/threats to:

- Confidentiality
- Integrity
- Availability

Take reasonable steps to reduce risk, and keep it low.

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 (P&P),
  - including on receiving complaints.
- Train workforce on HIPAA **&** entity's P&P.
- Develop a system of sanctions for employees who violate the entity's policies.
- Meet documentation requirements.

Major Impacts of Privacy and Security

New Patient Rights

- A written **notice** of information practices.
- Inspect and obtain a **copy** of their PHI.
- Obtain an **accounting** of disclosures.
- **Amend** their records.
- Accommodation of reasonable confidential **communication** requests.

Policies, Procedures, and Practices

- Must be documented and workforce trained on them.
- Agents and contractors must agree to protect health information under business associate agreements.

Security Required by Privacy

Enforcement Philosophy

Enforcement by investigating complaints.

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

Fines by HHS are unlikely (and small).

- Required by HIPAA to **help** people comply!

Fines and jail time possible from DOJ.

- Where intent can be proven.

BUT, real risk comes from

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

Strategically speaking, don’t wait around..

Participate!

Represent your sector in SDO meetings.

Monitor HIPAA rule making (listservs).

Respond to NPRMs:

- reasoned, practical advice to HHS ,
- about your environment.
- Personal responses as well as institutional.

Participate in efforts to share knowledge.

- WEDI and regional/national SNIP.
- Professional associations.

Attend/listen to NCVHS hearings.

- Read recommendations to HHS (web site).

Implement Ahead of Requirements

Primary focus on business drivers,

- secondary focus on regulatory drivers.

Implement philosophy first, then details:

- Information protection is an emerging business imperative.
- Remove system dependencies on identifier ‘intelligence’.

Standards based inter-system communication.

Make early decisions about electronic systems to meet documentation requirements:

- e.g., Disclosure accounting,
- Designated record sets,
- Acknowledgement tracking.

Implement Likely Regulations

Expected rules often transparent before final:

- Security rule,
- Transaction rule implementation guide addenda,
- NDC code requirement rescission, etc.

Implement as if you are COVERED ENTITY

- good BUSINESS ASSOCIATE practice;
- may fall under law in future (e.g., in Texas).

Hold sales force to products (e.g. policies) that can be supported by standards.

Don’t expect delays in privacy compliance dates.

Waiting until last minute always costs more than tweaking solutions implemented ‘at leisure’.

Understand & Control Your Data Flows

Cost savings in TCI

- Requires process re-engineering of data flows (and reduction of labor) to get most ROI.

Think about data flows and transactions not done electronically now:

- include them in strategic plans for future conversion.

Privacy, security:

- Inventory of data flow is one of first steps.
- Use hyperlinked data flow diagrams to educate, index, locate and maintain policies and procedures.

Consolidate Requirements

Approach enforcement from risk management philosophy:

- Good faith efforts and documentation are essential to demonstrate compliance.
- Find commonality in lower level implementation projects.

Structure of compliance effort:

- Privacy and security programs should be well coordinated (e.g., in an Information Protection program).
- Same structure, management team, and project support infrastructure:
  - Same mechanism to implement all training requirements.
  - Consider common responsibility & reporting – CPO, CSO.
  - Different experts and operational members.
- Integration of new programs into existing compliance effort.
- Partner with legal resources.

Enable Technology Flexibility

Rules will continue to be technology neutral

- Build/buy most cost-effective technology.

Standards based implementations save money

- Not a place to compete; proprietary solutions will cost more in end than the revenue they may generate by coercion.
- Participating in SDO activity can give years of warning.
- Consistent, system-wide APIs for services such as security allows flexibility and change without rewrites.
- Eases buy/build decisions.
- Easier integration of disparate systems.

Strategic Thinking Points

Participate in Rule Making

Implement Ahead of Requirements

Implement Likely Regulations

Understand & Control Your Data Flows

Consolidate Requirements

Enable Technology Flexibility

Don’t Do It All Alone

BE REASONABLE!

The Cost, Quality, Standards Relationship

Standards-based automation of routine functions lowers rate of rising costs (labor).

- Only possible if accompanied by process redesign.

Standardized data increases its usefulness for quality improvement studies.

  - Knowing what’s best can improve quality, but doesn’t prevent error.
  - 4th leading cause of death: medical errors!

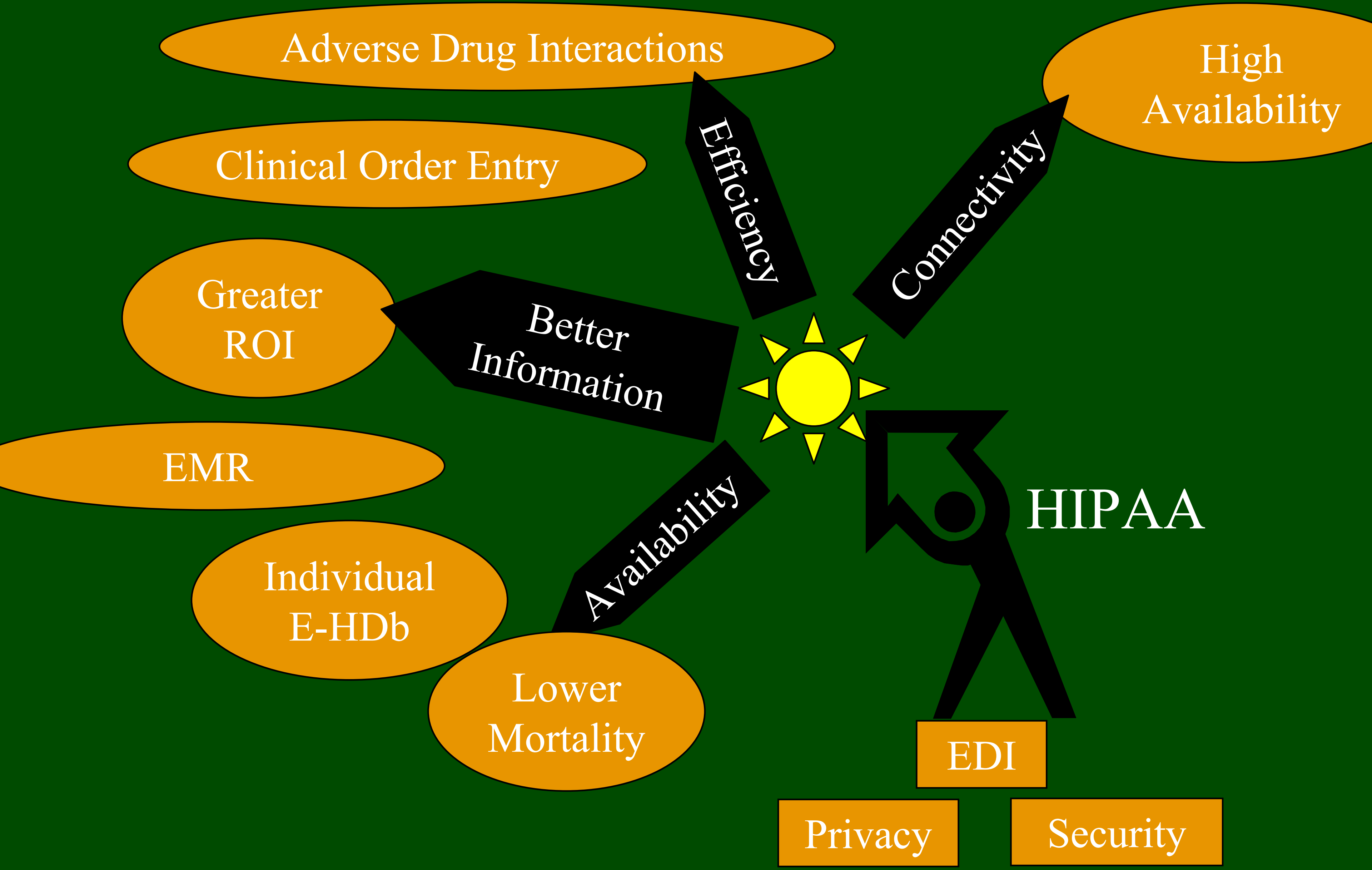
Standards for clinical information will allow more cost-effective introduction of IT support at point of clinical decision making.

- Which in turn, will lead to fewer errors, higher quality care, and lower costs (e.g. e-Rx, CPOE, EMR).
- NCVHS recommendations for PMRI standards.

The Future of HIPAA

Photo by Jay Kossman, P

Use HIPAA as a Catalyst for Change



PricewaterhouseCoopers

Resources

Centers for Medicare and Medicaid:

- www.hcfa.gov/hipaa/hipaahm.htm
- posting of regulations.
- instructions to join Listserv to receive e-mail notification of events related to HIPAA regulations.
- submission of rule interpretation questions (except privacy).

Office for Civil Rights:

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

Resources

National Committee on Vital and Health Statistics

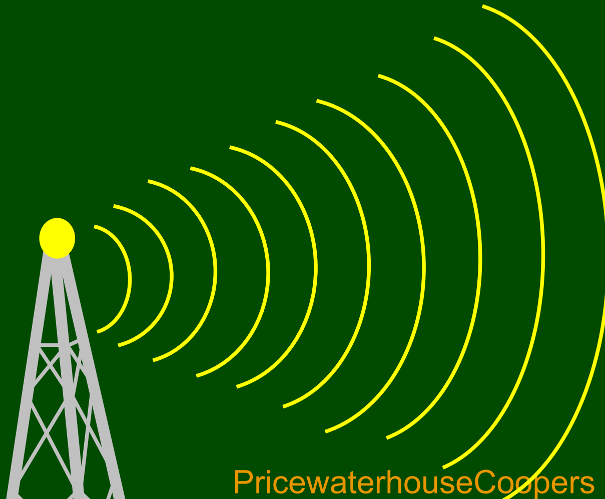
- ncvhs.hhs.gov

Workgroup on Electronic Data Interchange

- www.wedi.org
- snip.wedi.org

Other useful stuff:

- www.pwchealth.com/hipaa



Only 165 days left!

William.R.Braithwaite@us.PwCglobal.com

P W C

Your worlds Our people