Strategic Thinking in HIPAA Compliance

Administrative Simplification: Strategic Thinking in Compliance

William R. Braithwaite, MD, PhD
“Doctor HIPAA”
National HIPAA Summit
Washington, DC
April 25, 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 administrative 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.
Key Security Philosophy

Identify & assess risks/threats to:
- Availability
- Integrity
- Confidentiality

Take reasonable steps to reduce risk.

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 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.

Enforcement Philosophy

Preemption of state law wherever feasible.
- not politically possible for privacy.

Enforcement by investigating complaints.
- not HIPAA police force -- OCR not OIG.

“The Secretary will, to the extent practicable, seek the cooperation of covered entities in obtaining compliance”

The philosophy is to improve the health care system by helping entities comply, not by punishing unintentional mistakes.

Don’t wait around …

Participate in Rule Making

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,
• TCI addenda,
• NDC code requirement rescission, etc.

Implement as if you are COVERED ENTITY
• good BUSINESS ASSOCIATE practice;
• may fall under law in future.

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 to get most ROI.

Privacy, security
• Inventory of data flow is one of first steps

Think about data flows and transactions not done electronically now
• include them in strategic plans for future conversion

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 (information protection)
• 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 previous compliance efforts
• 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.

Strategic Thinking Points

Participate in Rule Making
Implement Ahead of Requirements
Implement Likely Regulations
Understand & Control Your Data Flows
Consolidate Requirements
Enable Technology Flexibility

BE REASONABLE!
The Cost, Quality, Standards Relationship

<table>
<thead>
<tr>
<th>Standards-based automation of routine functions lowers rate of rising costs (labor).</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Only possible if accompanied by process redesign.</td>
</tr>
<tr>
<td>• Could allow increased investment in clinical IT support.</td>
</tr>
</tbody>
</table>

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

**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).
- NCVHS recommendations for PMRI standards.

Resources

**Administrative Simplification Web Site:**
- [http://aspe.hhs.gov/admnsimp/](http://aspe.hhs.gov/admnsimp/)
  - posting of law, process, regulations, and comments.
  - instructions to join Listserv to receive e-mail notification of events related to HIPAA regulations.
  - submission of rule interpretation questions.

**Office for Civil Rights Web Site:**
- [http://www.hhs.gov/ocr/hipaa/](http://www.hhs.gov/ocr/hipaa/)
  - for privacy related questions.

**National Committee on Vital and Health Statistics**
- [ncvhs.hhs.gov](http://ncvhs.hhs.gov)

**Centers for Medicare and Medicaid**
- [www.hcfa.gov/hipaa/hipaahm.htm](http://www.hcfa.gov/hipaa/hipaahm.htm)

**Workgroup on Electronic Data Interchange**
- [www.wedi.org](http://www.wedi.org)
- [snip.wedi.org](http://snip.wedi.org)