Roundtable on Privacy in Transition: Is Privacy Policy Working in the Healthcare Sector?
The Sixteenth National HIPAA Summit: Special Edition

Gerry Hinkley, Moderator
Bill Braithwaite
Karen Grant
Deborah Peel
Michael Phillips~Linda Sanches~Jodi G. Daniel

Privacy Symposium SUMMER 2008
An Executive Education Program on Privacy and Data Security Policy and Practice
William R. "Bill" Braithwaite, MD, PhD, FACMI
Chief Medical Officer
Anakam Inc.
Washington, DC

Overview of HIPAA Privacy
Rule Principles and Issues
Principles of Fair Information Practice

- **Notice**
  - Existence and purpose of record-keeping systems must be 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**
  - Subject has right to see records and assure quality of information.

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

- **Enforcement**
  - Violations result in reasonable penalties and mitigation.
HIPAA Uses & Disclosures are Permissive

- **Required disclosures are limited to:**
  - Disclosures to the individual who is the subject of information.
  - Disclosures to HHS to determine compliance.
- **All other uses and disclosures in the Rule are permissive.**
- **Covered entities or states can provide greater protections if they want by preventing uses and disclosures that HIPAA allows.**
HIPAA Uses & Disclosures are Limited

- Limited to only what is permitted under 4 mechanisms in the Rule:
  1. Treatment, payment, and health care operations (TPO) after notice and acknowledgement.
  2. Uses and disclosures involving the individual’s care or directory assistance after opportunity to agree or object.
  3. Specific public policy exceptions.
  4. All others only when authorized by individual.

- Procedural requirements protect patient confidentiality based on type of use or disclosure.
Controversial Areas of HIPAA Privacy Rule

- Consent
- Minimum Necessary
- Disclosure Log
- Marketing
- Enforcement
- Preemption

Positions were arrived at after reviewing rationale of over 53,000 public comments.
e.g., the ‘Consent’ Debate

- One side: The information in the health record belongs to the patient. No information shall be used or disclosed to anyone without the explicit, informed consent of the patient.

- Another side: Such a demand cannot be supported in the current healthcare system. It would stop healthcare in its tracks. Others also have valid rights to use and disclose patient information under appropriate protections
  - legal business record of provider, documentation of work for reimbursement, documentation of quality for certification, public health reporting, research to improve medical knowledge that benefits us all, ...

- HIPAA was a compromise: informed by Notice of Privacy Practices, patient Choice is assumed for permitted, limited uses and disclosures when patients seek care.
New Privacy Issues

- **New record handling entities are not covered by HIPAA.**
  - Non-Covered Entities handling PHI in PHR and HIE
  - Banks handling PHI to pay medical expenses from HSA

- **New on-line services are not addressed.**
  - BA chain to off-shore services
  - Marketing banners and pop-ups relating to PHI

- **New security risks must be countered.**
  - Increasing theft of portable media and devices
  - Use of health information for identity theft

- **New technology must be considered.**
  - Could enable patients to have more control of their information

- **New Laws must be monitored and complied with.**
  - Federal v. State law
  - Regulations
Karen G. Grant
Corporate Director, Health
Information Services

Partners Healthcare System, Inc.

A Provider’s Perspective
Principles:

Minimum Necessary
Appropriate Access to Appropriate information at the appropriate time
ROI strictly within state and federal requirements
Patient access (access rights and “customer service”)
Data integrity

How: Training, Policies, Trust

Patients are notified of the organizations practices
Employees and clinicians are educated
Disciplinary action
Awareness
Technology

- Technology can support this vs. technology can hurt if the fundamental principles are not in the forefront.
- Support via Access-Passwords
- Support via Restrictions
- Technology can help e.g. identification of who accessed information (but don’t forget in a paper or hybrid system requirements for “audits” or monitoring may be beyond the capability of the organization).
- Active use of passwords or similar protection a must.
- Encryption used where ever feasible.

Why is it hard/Why is it worth it.........................
Challenges

The above principles are important why is it so hard....

- The reality is large busy medical centers need information when the need it to treat patients
- The health care industry with it's limited resources not easy to obtain consents and discuss notices
- Applications will run slowly because of need to know checks
- Balancing taking care of a patient vs. meetings on privacy
- There can be reasonable disagreements about the steps to protect privacy
- Definitions are murky
- New dangers i.e. identity theft
Challenges

Why is it worth it

- We don't want to harm our patients by erring on the side of restriction
- We want our patients to trust us with their information
- We understand there can be lasting damage if info is released inappropriately
Deborah C. Peel, M.D.
Founder and Chair
Patient Privacy Rights
Coalition for Patient Privacy

The Consumer Perspective
President Bush implemented the HHS HIPAA “Privacy Rule” which recognized the “right of consent”.

1996 Congress passed HIPAA, but did not pass a federal medical privacy statute, so the Dept. of Health and Human Services (HHS) was required to develop regulations that specified patients’ rights to health privacy.

2001 President Bush implemented the HHS HIPAA “Privacy Rule” which recognized the “right of consent”.

2002 HHS amended the HIPAA “Privacy Rule”, eliminating the “right of consent”.

“…the Secretary of Health and Human Services shall submit to [Congress]…detailed recommendations on standards with respect to the privacy of individually identifiable health information.”

“….a covered health care provider must obtain the individual’s consent, in accordance with this section, prior to using or disclosing protected health information to carry out treatment, payment, or health care operations.”

“The consent provisions…are replaced with a new provision…that provides regulatory permission for covered entities to use and disclose protected health information for treatment, payment, healthcare operations.”
What does ‘privacy’ mean?

- The NCVHS (June 2006, Report to Sec. Leavitt) defined health information privacy as “an individual’s right to control the acquisition, uses, or disclosures of his or her identifiable health data”. (Definition originally from the IOM)
“Anyone today who thinks the privacy issue has peaked is greatly mistaken…we are in the early stages of a sweeping change in attitudes that will fuel political battles and put once-routine business practices under the microscope.”

Forrester Research

an independent technology and market company that provides advice to global leaders in business and technology
Linda Sanches  
Senior Advisor  
HIPAA Privacy Outreach & Training  
Office of Civil Rights  
U.S. Dept. Health & Human Services  

Michael Phillips  
Health Insurance Specialist  
Office of E-Health Standards and Services  
CMS  

Jodi G. Daniel  
Director, Office of Policy and Research  
Office of the National Coordinator for Health Information Technology  

HHS's Perspective
Questions for the Panel