What are the Key HIPAA Privacy Compliance Challenges Today and in the Future?

December 12, 2007

Bill Braithwaite, MD, PhD
Health Information Policy Consulting
Washington, DC

Principles of Fair Information Practice

- ***Notice***
  - The existence and purpose of record-keeping systems must be known to the individuals who are the subjects of the records.
- ***Choice***
  - Information must be collected only with the knowledge and implicit or explicit permission of the subject, used only in ways relevant to the purpose for which the data was collected, and disclosed only with permission of the subject or in accordance with overriding legal authority (such as a public health law that requires reporting of a serious contagious disease).
- ***Access***
  - Individuals must have the right to see records of information about them and to assure the quality of that information (accuracy, completeness, and timeliness). In healthcare, records are rarely deleted or replaced, but this principle implies that there is at least a due process for individuals to amend poor quality information about them.
- ***Security***
  - Reasonable safeguards must be in place for the confidentiality, integrity, and availability of information.
- ***Enforcement***
  - Violations must result in reasonable and consistently applied penalties to deter violators and in reasonable mitigation efforts to offset the effects of a breach.

HIPAA is the Floor

- HIPAA Privacy Rule considers all personal health information equally sensitive.
  - HIPAA permits patient health information to be used and disclosed for treatment, payment, and health care operations without patient consent.
  - Some state laws require patient consent even for treatment purposes.
  - A variety of federal and state statutes and regulations (laws) afford heightened privacy protections for certain classes of information generally perceived as sensitive and requiring special protections.

Federal Preemption by HIPAA

- The HIPAA regulations preempt contrary provisions of State law
  - except where State law provides a more stringent (higher) privacy standard.
- Applicability of other federal laws is NOT affected.
  - Resulting in complex web of regulations from federal, state, and local law.

HISPC Sources of Variation

- Variation related to misunderstandings and differing applications of federal laws and regulations:
  - HIPAA Privacy Rule
    - Confusion about Patient Authorization/Consent
    - Variation in Determining “Minimum Necessary”
  - HIPAA Security Rule
    - Confusion regarding the different types of security required
    - Misunderstandings regarding what was currently technically available and scalable
  - CFR 42 part 2
    - Variation in the understanding of treatment facilities, physicians, and integrated delivery systems of 42 C.F.R. pt. 2, its relation to HIPAA, and the application of each regulation

HISPC Sources of Variation (continued)

- Variation related to state privacy laws
  - Scattered throughout many chapters of law
  - When found, they are sometimes conflicting
  - Often antiquated – written for a paper-based system
- Trust in applied information security
  - Organizations mistrust each other
  - Consumers/Patients mistrust organizations (except their doctors)
- Cultural and business issues
  - Concern about liability for incidental or inappropriate disclosures
  - General resistance to change

HISPC Summary

- Variations in privacy and security practices will impede HIE and HIT Initiatives unless resolved.
- GAO Challenges from June 2007 Report are similar.
- States are starting to understand the issues.
- States are formulating solutions:
  - Practice and Policy Solutions.
  - Legal and Regulatory Solutions.
  - Technology and Data Standards.
  - Education and Outreach.

- Multi-state and National Level Recommendations are forthcoming.

Alternatives to Consider (continued)

- **Federal Law Modifying HIPAA**.
  - A law that adds new types of organizations that handle individually identifiable health information would require new regulations applying principles to new functions.
  - Including requirements for specific clinical information transaction standards could justify covering new entities.
  - Classifying eHIE organizations as a new type of health care clearinghouse.
  - Classifying PHR services as covered entities because of their direct interactions with patients.
- **Statutory approaches** that states could adopt to resolve conflicts between state laws governing consent:
  - uniform state law,
  - model state law,
  - choice of law provisions, and
  - interstate compact.

Alternatives to Consider

- **New Comprehensive Federal Law.**
  - covers all participants equally but difficult to get passed.
  - different types could address these issues:
    - **Non-discrimination law**. – Making it illegal for organizations to discriminate against individuals based on their health status would remove the major motivation for people to keep their health information secret, making the rest easier to handle.
    - **Comprehensive privacy law**. – Requiring each state to pass laws that meet certain criteria based on the principles of fair information practice; states that signed up for such an approach could not send individually identifiable data to states that had not signed up.
    - **Comprehensive health information privacy law**. – A law like the one that was promised by HIPAA would apply to any person who handles the individually identifiable health information of another person, and would limit state variability to enable eHIE.

Greatest Compliance Challenges

1. Engendering trust.
   - Lack of trust endangers interoperable HIE.
2. Following laws and regulations, today and in the future.
   - Harmonizing state laws & regulations.
   - Normalizing business practices (policies and procedures).
   - OCR is hiring again.
3. Linking patient records.
4. Educating patients and providers.
   - Consumer expectations.
   - Provider fear, uncertainty, and doubt.

1. Engendering Trust is THE Challenge

- Trust is a critical issue that affects the viability of electronic HIE.
- Trust (or lack of it) leads organizations to draft extremely conservative policies that contribute to the variation in business practice and policy which in turn forms a barrier to HIE.
- Trust can be built over time by meeting and learning about the issues and views of other stakeholders.
  - It takes time and personal contact.

‘Consent’ is a Major Issue in Trust

- Wide variation among organizations in practices and policies that determine when patient permission is required, how the permission is obtained and documented, and how patient permission is communicated to health care organizations, payers, and other outside entities.
- Variation caused by a number of factors, including:
  - a basic misunderstanding of whether and when the HIPAA Privacy Rule required patient permission to disclose health information, particularly with respect to treatment;
  - confusion over the terms used for the process for obtaining patient permission;
  - federal and state laws with patient permission standards that differed from the HIPAA Privacy Rule, particularly those that applied to *specially protected health information*; and
  - organizational decisions to require patient permission as an added protection to reduce risk of liability for wrongful disclosure.

‘Consent’ is a Major Issue in Trust

- Consumers are concerned about how their health information is being managed, used, and disclosed electronically by providers, payers, researchers, and emerging HIEs and regional health information organizations (RHIOs).
- Providers are concerned about the appropriate interpretation of state laws related to consent for release of health information issues and the potential risks or liabilities associated with their failure to comply with such laws.

The ‘Consent’ Debate Frame

- **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.

Complexity of Consent

- Need to be able to distinguish between consent, authorization, and permission as concepts and decide on how to use each in this process.
  - Does the motivation of the patient wanting to keep information secret affect the process or the data collected when asking for permission to share health information? For example, is there a difference between wanting to keep health information secret to avoid discrimination and just wanting information to be ‘private’ from people you might know?
  - What is the rationale for requiring permission to use and disclose health information for treatment purposes (and perhaps also for payment and healthcare operations) in light of ‘assumed permission’ position of HIPAA?
  - What criteria should be the basis of decisions as to process and data content for getting patient permission under different circumstances. How can obtaining permission and the data collected in a standardized, meaningful process meet the requirements of all these situations?

Definition and Granularity

- **Types of information** – For example, how do you define what is ‘sensitive’ information?” Are there multiple types of ‘sensitive’ information deserving different treatment? Is different information ‘sensitive’ for different people? How do you identify it? Is permission required to use or disclose de-identified information?
- **Purpose of information** – For example, are disclosures for payment purposes to be treated differently than disclosures for treatment?
- **Routes of disclosure** – For example, are disclosures for treatment purposes treated the same whether they are conducted provider-to-provider, through a third party, or through an HIE?
- **Permission process** – Is the process of data collection different when obtaining permission in an opt-in situation as opposed to an opt-out situation? Can a disclosure be made to the HIE on basis of a BA contract without permission as long as no disclosures are made by the HIE without appropriate permission? Is the process different for different classes of disclosures?
- **Secondary disclosures** – Under what conditions should limitations be imposed on secondary uses and disclosures?
- **Emergency access** – Under what conditions may we disregard the patient’s restrictions on sharing information? For example, how do we define ‘emergency’ and what process should be used to “break the glass” in an emergency?
- **Harmonization** – How will the process and data collection deal with inconsistencies and overlap between multiple federal laws, state and local laws, and business practices?

2. Harmonizing with Changing Laws

- A high level of variation exists in states' approaches to issues of health privacy. Even within individual states, variation in the understanding of and approach to health privacy is still prevalent.
- The challenge is to synchronize the update of laws from multiple states to ensure privacy while facilitating the interoperability of HIE.
- Variable business practices must be harmonized and kept in synch with changing legal requirements.

3. Linking Patient Records

- Variability in methods across organizations to link patients to records, and the lack of agreed-upon patient-to-record matching standards to apply when interorganizational electronic HIE is conducted.
- Concern about liability for incidental or inappropriate disclosures causes many to take a conservative approach.
- Clinicians believe it is ‘safer’ to make do with less information on a patient where there is any question about identity, rather than to potentially base clinical decisions on information from the wrong patient.
- The challenge is to reach agreement on how to preserve confidentiality while accurately linking patient records from different sources without a national patient identifier.

4. Educating patients and providers

- Variations in state laws, both intrastate and interstate, must be understood before the states can work toward a common framework more hospitable to interoperable HIE.
- Educational programs must address demonstrated gaps in knowledge such as differing interpretations of HIPAA and the perceived privacy and security dangers of interoperability.
- Successful education and engagement requires that consumers, providers, educators, and other stakeholders have a common and correct understanding of terms.
- Getting the time and attention of both providers and patients to participate is a serious challenge.

Conclusion

- Variations in privacy and security practices will impede HIE and HIT Initiatives unless resolved.
- Current laws and regulations are variable, complex, and poorly enforced – states are making changes.
- Current business practices and inconsistent, variable, and not based on reasonable interpretations of principle or law.
- Compliance challenges are long-term and interdependent:
  - Laws are in flux.
  - Consent issues have not been resolved.
  - Record matching standards have not been set.
  - Education has been inconsistent and inadequate.
  - Trust must be earned.

Questions?

Bill@Braithwaites.com