Recent Developments for Best Practices for Privacy in Health Information Exchange – A Legal View

Allen Briskin
Counsel
Pillsbury Winthrop Shaw Pittman
allen.briskin@pillsburylaw.com
July 14, 2011

Issues

- Direct regulation of HIEOs as business associates
- Federal and state data breach reporting requirements
- Updating Business Associate Agreements
- Changing rules regarding accountings of disclosures
- Focus on ACOs driving functionality demands
- Exchanging information outside the HIEO, *e.g.*, HIEO to HIEO exchange
- Liability (and insurance & indemnification)

Direct Regulation & Data Breach Notification

- HITECH Act
  - Expressly provides that those providing data transmission of PHI for covered entities are business associates
  - Subjects business associates to direct regulation under HIPAA & HITECH
  - Subjects covered entities to federal data breach notification requirements, thus demanding corresponding obligations of business associates
- State law developing regarding identity theft & data breach reporting and/or notification requirements for health and other information
- HIEOs may need to update their business associate agreements
- Simplifying the process
- Moving to scale back or eliminate the business associate agreement requirement

Updating Business Associate Agreements

- Tendency to impose unnecessarily burdensome requirements
- Consider whether flexibility and collaboration may be a better model for the covered entity – business associate relationship
- Example: Responding to "Security Incidents"
  - Attempted or successful unauthorized access, use, disclosure, modification or destruction of information, or interference with system operations in an information system
  - Unsuccessful attempts to interfere with security or operations require a response
  - Business associates must identify, track, mitigate and document security incidents, and report to covered entity security incidents of which they become aware
  - Compare: report each security incident within 2 days vs. prepare periodic report of unsuccessful security incidents and report the others within a more reasonable period of time
  - Response time should be directed toward covered entity's regulatory needs

Accountings of Disclosures; Access Reports

- HIPAA requires individuals receive accountings of disclosures upon request
- HITECH expanded the requirements to include disclosures for treatment, payment & health care operations
- HHS proposes new rules seen as effort to ease compliance
- Scaled back accountings requirements, but added access report requirements
- Compliance with access report rules required by 1/1/2013 (for systems acquired after 1/1/2009) or 1/1/2014 (for systems acquired earlier)
- Concerns about technological and other resources required for compliance and useful implementation
- Comment period ends 8/31/2011

Developing Functionality Demands, *e.g.*, ACOs

- Patient Protection and Affordable Care Act ("ACA") creates Medicare Shared Savings Program ("MSSP") to allow accountable care organizations ("ACOs") to contract with Medicare to "be accountable for the quality, cost, and overall care of Medicare beneficiaries . . . who are assigned to it."
- Even if ACOs do not get off the ground, some expect that the commercial market will drive development of ACOs or ACO "look-alikes"
- ACOs must meet quality, etc. standards in five "domains" (patient/care giver experience, care coordination, patient safety, preventive health, at-risk populations)
- Information systems subset of care coordination domain drives ACO physician's achievement of meaningful use of EHR technology, use of clinical decision support, e-prescribing and patient registry use
- ACO physicians will rely on HIEO to achieve necessary degree of care coordination
- Examining technology and services to meet resulting functionality demands

Exchange of Information Outside the HIEO

- Provision of information to non-HIEO participants
- Exchange of data with other HIEOs and/or their participants
- Harmonizing privacy, security and other policies and procedures
- Looking for external and/or impartial guidance for decision-making and dispute resolution (*e.g.*, New York's Statewide Policy Guidance)
- Revisiting HIEO role in enforcement of participants' obligations

Liability Concerns

- Concern regarding harm from system failures or use failures, and resulting lawsuits caused by “the other guy’s” negligence, etc.
- Hypothetical agreement to standard indemnification requirements, *i.e.*, each is responsible for her own
- Agreement for all to obtain insurance
- With implementation, and change to existing work flows and practices, new concerns emerge
- Push to build standard of practice into HIEO documents
- Managing the HIEO’s role regarding establishment and/or enforcement of standard of practice
- Considering expansion of participant-to-participant obligations

Questions & Comments

Allen Briskin

Counsel

Pillsbury Winthrop Shaw Pittman

allen.briskin@pillsburylaw.com

pillsbury