Privacy and Security in Mini-Sentinel: Ensuring Public Trust through Respectful Use of Health Information

Kristen B. Rosati
Coppersmith Schermer & Brockelman, PLC

Engelberg Center for Health Care Reform at Brookings Sentinel Initiative Public Workshop
January 12, 2011
Agenda

- Data flow in the Mini-Sentinel pilot
- Legal compliance
- Policies that reflect fair information practices

The Mini-Sentinel Privacy Panel:
- Deven McGraw, Director, Health Privacy Project, Center for Democracy & Technology
- Barbara Evans, Associate Professor, Co-director, Health Law & Policy Institute, Director, Center on Biotechnology & Law, University of Houston Law Center
- Kristen Rosati, Partner, Coppersmith Schermer & Brockelman PLC
Mini-Sentinel Distributed Analysis

1. FDA
2. Mini-Sentinel Portal
3. Data Partner Firewall / Policies
   - Review & Run Program
4. Local Datasets
5. Operations Center
   - Review & Return Results
Data Flow in Mini-Sentinel

- Distributed Data Model: Data Partners maintain physical and operational control over the original source data and data is transformed into the Mini-Sentinel Common Data Model (MSCDM) format
  - Operations Center sends standardized queries to Data Partners
  - Data Partners execute queries against data in the MSCDM format and share summary results with Operations Center
  - Data Partners may be asked to provide non-summary, patient-level information as follow-up, but will strip out direct patient identifiers before disclosure to Operations Center
Data Flow in Mini-Sentinel

- If Data Partners do not maintain original source data, they may ask data source for medical records to further analyze drug safety signal; Data Partners will ensure that direct patient identifiers are redacted before sending to Operations Center
Health Insurance Portability and Accountability Act (HIPAA)

- HIPAA permits disclosure of protected health information (PHI) to a “public health authority” for public health surveillance (which includes the safety of FDA-approved products)
  - FDA is a public health authority
  - Public health authority also includes a “person or entity acting under a grant of authority from or contract with such public agency” – Mini-Sentinel Operations Center and its subcontractors are acting under a grant of authority from the FDA
- Release of PHI (if any) to the Data Partners, the Operations Center and the FDA is not for “research” that requires approval by an Institutional Review Board

krosati@csblaw.com
Federal Substance Abuse Treatment Regulations (the “Part 2 Regulations”)  

- Part 2 regulations protect information generated by a federally-assisted alcohol or drug abuse treatment program, if the information identifies a patient as an alcohol or drug abuser or someone who has applied for or received that type of treatment.

- Part 2 regulations are unlikely to affect Sentinel, but covered data sources will need to evaluate release of original source data to Data Partners for analysis.
State Confidentiality Laws

- State health information confidentiality laws often provide more protection for “special” health information, such as:
  - Genetic testing
  - Mental health information
  - HIV/communicable diseases
- Most state laws regulate external disclosure, but not internal use of health information
- Many state laws permit release for public health activities
- No state laws (to my knowledge) regulate the release of aggregated, non-identifiable information
- Each data source will need to confirm compliance with its own state laws
Fair Information Practices

- Data Integrity and Quality
- Collection and Use Limitations
- Purpose Specification and Minimization
- Openness and Transparency
- Individual Participation
- Security Safeguards and Controls
- Accountability and Oversight
Policies Comply with Fair Information Practices

- Distributed data model: drug safety questions are brought to the data
- All direct identifiers are removed from information provided to the Operations Center or the FDA
- Any identifiable information received by Data Partners to confirm drug safety signals is used only for Mini-Sentinel purposes
- Operations Center may use information it receives only for Mini-Sentinel purposes
- Operations Center manages security in accordance with the HIPAA Security Rule and the Federal Information Security Management Act
Thank you!

Kristen B. Rosati
Coppersmith Schermer & Brockelman PLC
2800 North Central Avenue, Suite 1200
Phoenix, Arizona 85004
tel (602) 381-5464/fax (602) 772-3764
Email: krosati@csblaw.com
www.csblaw.com