



Sonnenschein

**COMMUNITY-BASED
COLLABORATIONS:
Legal Issues In Structuring Health
Information Exchanges**

**The Health Information Technology Summit
October 23, 2004**

**Reece Hirsch
Sonnenschein Nath & Rosenthal LLP
San Francisco, CA (415)882-5040
rhirsch@sonnenschein.com**

Health Information Exchanges Are Local

- Like health care generally, a health information exchange is a local enterprise.
- Unique state law considerations
- Exchanges can take many forms
 - Peer-to-peer systems
 - Facilitating financial transactions
 - Clinical data repositories

Health Information Exchanges Are Local

- Review of legal issues that generally apply to exchanges, regardless of structure or locality
- Devil is in the details – and the details involve state law

Governance and Organization

- **Early discussions**
- **Statement of Purpose and Objective**
- **Memorandum of Understanding**
 - **Entity's purpose and objective**
 - **Which organizations may participate in network**
 - **How network's efforts will be funded**
 - **Potential liabilities**
 - **How the network will be governed and operated**

Governance and Organization

- **Initial structure**
 - **Tax status**
 - **Board composition**
- **Sources of funding**
 - **eHealth Initiative sub-grants to communities as part of “Connecting Communities for Better Health” initiative**
 - **Health plans**

Governance and Organization

- **Testing the waters**
 - **Health information exchange may be organized more simply during beta test stage**
 - **Adding a broader range of participating organizations and functions after beta stage**

Governance and Organization

- **Someone has to be in Charge**
- **Corporate Formation and Tax Status**
- **Governance**
- **Creating a Business Plan and Budget**
- **Sources of Revenue**
- **Criteria for Involvement**

Tax Status

- Is a health information exchange “organized and operated exclusively for charitable and educational purposes” under IRC Section 501(c)(3)?
- Must distinguish IRS private letter rulings regarding 501(c)(6) organizations or “business leagues,” such as medical societies

Tax Status

- **Factors that will favor tax-exempt status:**
 - **Control by community board**
 - **Improvement in delivery and access to health care services**
 - **Broad sources of support**
 - **Open participation**
 - **Exchange is not solely intended to further the common business interests of participants**

Tax Status

- Revenue Ruling 76-455
 - “A nonprofit organization formed to encourage and assist in the establishment of nonprofit regional health data systems ... is operated exclusively for scientific and educational purposes,” and thus qualifies for 501(c)(3) status
 - Activities were “not carried on to set standards for or to police the industry but to provide ... benefits to the general public.”

Vendor Agreements

- Agreements between the Exchange Entity and IT and other vendors
- Detail operational and performance specifications for both vendor and entity
- Performance measurements and rewards and penalties
- Specify key staff
- Audit rights and protocols
- Compliance with HIPAA and other regulations
- Compensation
- Intellectual property issues

HIPAA Relationships in a “Hub and Spokes” Health Information Consortium

- **Members of the Consortium are covered entities under HIPAA**
- **The hub organization is not a covered entity unless it converts standard transactions and functions as a health care clearinghouse**
- **The hub organization is a business associate of each member of the Consortium – business associate provisions should be included in each user agreement between members and the hub organization**
- **The members are not business associates of one another -- the members are not providing services to or on behalf of one another**

Oversight of Hub Organization and its Vendor by Consortium Members

- HIPAA does not technically require affirmative oversight by covered entities of their business associates – representations in business associate agreements are legally sufficient
- Covered entities are liable for privacy breaches of business associates only if they know of an improper pattern of activity or practice and fail to take appropriate action
- But higher level of oversight may be imposed in practice given the amount of data concentrated in a single location and the highly structured nature of the enterprise
- There may be opportunities for Consortium members to jointly perform privacy and security oversight of the hub organization or its vendor through a mutually selected agent

Key Privacy Screens for Data Access Requests

- Is patient authorization required for access?
- If so, did the patient provide sufficient authorization?
- If not, is the party requesting the “minimum necessary” information for the intended purpose?
- Has the data holder agreed to a restriction on uses?
- Does the party requesting the data have a treatment or coverage relationship with the patient?
- Is the party requesting the data who they say they are?

Is Patient Authorization Required for Access?

- HIPAA has liberal rule that permits disclosure without *authorization* for treatment, payment and health care operations – this will cover almost all disclosures among Consortium members
- Consider whether patient *consent* may be appropriate from risk management standpoint before sharing the patient's data electronically through the Consortium
 - However, patient consent can be a major operational stumbling block

Health Care Operations

- If health information exchange is generating various outcomes and utilization reports for participants, may qualify as “health care operations” under HIPAA, which include:
 - Quality assessment and improvement, outcomes evaluation, case management and care coordination, evaluating provider or health plan performance and population-based activities relating to improving health or reducing health care costs

Is Patient Authorization Required for Access?

- State confidentiality laws may also require authorization and are likely to pose the greatest challenge:
 - often more stringent consent requirements than HIPAA
 - requirements vary with the type of information (e.g., HIV/AIDS, mental health, Medicaid)
 - separate laws may have differing consent requirements (oral vs. written, required elements, etc.)
 - laws may be applicable only to a subset of Consortium members (e.g., insurers, hospitals, mental health facilities, public agencies)
- Federal regulations governing substance abuse treatment records are also more stringent than HIPAA

State Law Challenges

- In working with a California data exchanges, particular challenges were posed by participants that were:
 - “Agencies” subject to Cal. Information Practices Act of 1977
 - “State and local agencies” subject to California Public Records Act
 - An agency engaged in administration of the Medi-Cal program (Section 14100.2 of Cal. Welfare & Institutions Code)

Veteran's Administration

- If a VA hospital or clinic participates in the exchange, issues under the federal Privacy Act of 1974 may apply
- When a VA agency provides by contract for the operation of a system of records to accomplish an agency function, Privacy Act applies to the system
- Health information exchange may not be a VA “system of records” because if it is not “under the control” of the VA

Is the Party Requesting the Minimum Necessary Information?

- HIPAA requires covered entities to *request* the minimum necessary information for the intended purpose
- If Consortium consists exclusively of covered entities, each party disclosing data may rely on the requesting party's minimum necessary determination if reliance "is reasonable under the circumstances"
- Other minimum necessary exceptions may also apply:
 - Disclosures to providers for treatment
 - Disclosures to the patient or pursuant to the patient's authorization
- Minimum necessary rules can also be embedded in system

Has the Data Holder Agreed to Restrict Uses?

- HIPAA allows patients to request restrictions on uses of data for treatment, payment or health care operations
- Covered entities do not have to agree to all restriction requests
- Data holders must have the capacity to override otherwise permissible access requests based on agreed upon restrictions
 - Or data holders must all agree that it is not their practice to agree to restrictions

Does the Requesting Party Have a Relationship with the Patient?

- Health care providers and health plans are not entitled to data on any person without regard to whether there is a treatment or coverage relationship
- Centralized system enabling each provider and plan to verify and register their relationships with patients can avoid case-by-case verification
- May elect “break the glass” capability for emergency situations, subject to back-end audit

Is the Requesting Party Who They Say They Are?

- HIPAA requires covered entities to verify identity of parties receiving protected health information
- Assignment of unique user ID and password by hub organization will be required
- Use of digital certificates may be warranted

Consortium Must Perform Security Risk Analysis

- Great importance placed on risk analysis in HIPAA Security Rule
 - Underlies decisions regarding all “addressable” specifications
 - Basis for selecting competing security options
 - Integral to making scalability decisions related to compliance
- Sophisticated risk analysis would be expected for this type of venture
- Each Consortium member may rely on the risk analysis performed centrally by the Consortium or its vendor – but internal review of the analysis by a member may be appropriate, depending on its size and resources

Hub Organization Responsible for Network Security Issues

- Encryption – this is an “addressable” standard but a risk analysis is likely to identify this as a necessary measure for any internet-based transmission (encryption of stored data may be deemed appropriate as well)
- Audit trail – required for privacy and security monitoring and could assist in meeting accounting of disclosures mandate
- Authentication – issuance of unique user IDs and passwords, and digital certificates if utilized
- Physical safeguards in data center (access control, environmental control, emergency power, disaster recovery plan, etc.)

Consortium Members Not Relieved of Own Security Responsibilities

- Workforce clearance and termination procedures
- Role-based access controls
- Virus protection
- Data back-up
- Device and media controls
- Physical safeguards

Consortium May Set Minimum Security Standards for Each Member

- Standards may be scalable based on size and resources of members
- Minimum standards may be included in user agreements
- Consortium may audit compliance by each member

Security Training May be Shared Responsibility

- Hub organization may develop curriculum
- Hub organization may use “train the trainer” model or conduct training of all users
- Division of training responsibility may depend on size and sophistication of individual members
- Evidence of training should be maintained by each member



Sonnenschein

For further information contact:

Reece Hirsch

Sonnenschein Nath & Rosenthal

415.882.5040

rhirsch@sonnenschein.com