GET CONNECTED KNOWLEDGE FORUM

LEGAL ISSUES
IN
GETTING COMMUNITIES CONNECTED
JUNE 28, 2005

Paul T. Smith, Esq.
Partner, Davis Wright Tremaine LLP
One Embarcadero Center, Suite 600
San Francisco, CA 94111
415.276.6532
paulsmith@dwt.com

Regional Health Information Organization

Public health surveillance
Quality accountability

Research

Health Plan

RHIO

Provider

Provider

Provider

Provider

Consumers
Consumer Participation

- NHII—
  - "Consumer-centric"
  - Includes a personal health record
  - Has a strong theme of consumer "ownership"
- Consumer consent not required for inclusion in RHIO by provider, as long as there are

Consumer Control

- Many advocate an "opt-in" model
- What rights should the consumer have to—
  - Control data going into the NHII?
  - Control access to that data?
- What are the implications for providers?
What uses and disclosures are permitted?

- HIPAA is permissive: the only required disclosures are to
  - The individual
  - HHS for HIPAA compliance investigation
- Treatment is a given, but what are the rules for—
  - Health care operations, including payment
  - Public health oversight
  - Research
- Use by law enforcement

Security in a RHIO

Covered entities must maintain reasonable and appropriate administrative, technical and physical safeguards—

- To ensure confidentiality and integrity of information
- To protect against reasonably anticipated--
Security in a RHIO

- Basic requirements with implementation features
- Technology neutral, flexible and scalable
- To be implemented in a manner that best suits the entity's needs, circumstances and resources, taking into account
  - Size, complexity and capabilities
  - Technical infrastructure and capabilities
  - Cost of security measures
  - Potential risks to health information

Security in a RHIO

What is missing?

- Clearly defined, uniform security requirements
- Access restrictions
  - Authentication with non-repudiation
- Technical restrictions on use
- Audit trials
- Enforcement, enforcement, enforcement
Policing the RHIO

- Not directly regulated
- Covered entities disclosing health information are required to obtain & enforce contractual assurances that the RHIO will--
  - Safeguard the data (security)
  - Restrict uses and disclosures to those permitted to the covered entity (privacy)
  - Return or destroy the data on termination, if feasible

Policing the RHIO

- A covered entity is liable for breaches by business associate if the covered entity--
  - Learns of a pattern or practice of violations, and
  - Fails to take reasonable and appropriate remedial measures
- Weak standard
User Agreements - Structure

- Policies and Procedures
  - Can be changed on notice with user opt-out
- Core terms
  - Common terms
  - Role-specific terms
- User agreement
  - Designates user's role
  - Incorporates core terms and P&Ps

User Agreements – Policies & Procedures

- User enrollment and termination
- Technical requirements
- Data standards
- Security requirements
- Privacy practices (permitted uses)
- Consumer rights
User Agreements – Core Terms

- Ownership of system and data
- Nature of user's right to use
- Permitted uses, based on user's role

User Agreements – Core Terms

- User’s responsibilities:
  - Compliance with policies and procedures
  - Accuracy and completeness of contributed data
  - Appropriate authorizations/NPPs
  - Payment of fees
User Agreements – Core Terms

- Network’s responsibilities:
  - Maintain and support the system
  - Maintain privacy and security of data
  - Credential users
  - Police the system
  - Afford individual rights

User Agreements – Core Terms

- Fees and charges
- Disclaimers, limitations and indemnifications
- Term and termination provisions
  - What happens to the data?
User Agreements – Individual Agreements

❖ Identify user

❖ Identify user’s role

❖ Incorporate core terms and P&Ps