FOURTH HEALTH INFORMATION TECHNOLOGY SUMMIT

LEGAL ISSUES IN HEALTH INFORMTION TECHNOLOGY

MARCH 29, 2007

Paul T. Smith, Esq.
Partner, Davis Wright Tremaine LLP
505 Montgomery St., Suite 600
San Francisco, CA 94111
415.276.6532
paulsmith@dwt.com

Topics

- Consumer Rights
- Privacy
- Security
- Electronic Health Record
- Medical Liability Risks

National Health Information Infrastructure

- Executive Order 1335, April, 2004—
  - Called for widespread adoption of interoperable EHRs within 10 years
  - Created position of National Coordinator for Health Information Technology
  - National Coordinator issued a Framework for Strategic Action issued July 21, 2004
  - Consists of 4 goals, each with 3 strategies

Goals of the NHII

- Informing Clinical Practice
  - Promoting use of EHRs by
    - Incentivizing EHR adoption
    - Reducing the risk of EHR investment

Goals of the NHII

- Interconnecting clinicians by creating interoperability through
  - Regional health information exchanges
  - National health information infrastructure
  - Coordinating federal health information systems

Goals of the NHII

- Personalizing care
  - Promotion of personal health records
  - Enhancing consumer choice by providing information about institutions and clinicians
  - Promoting tele-health in rural and underserved areas

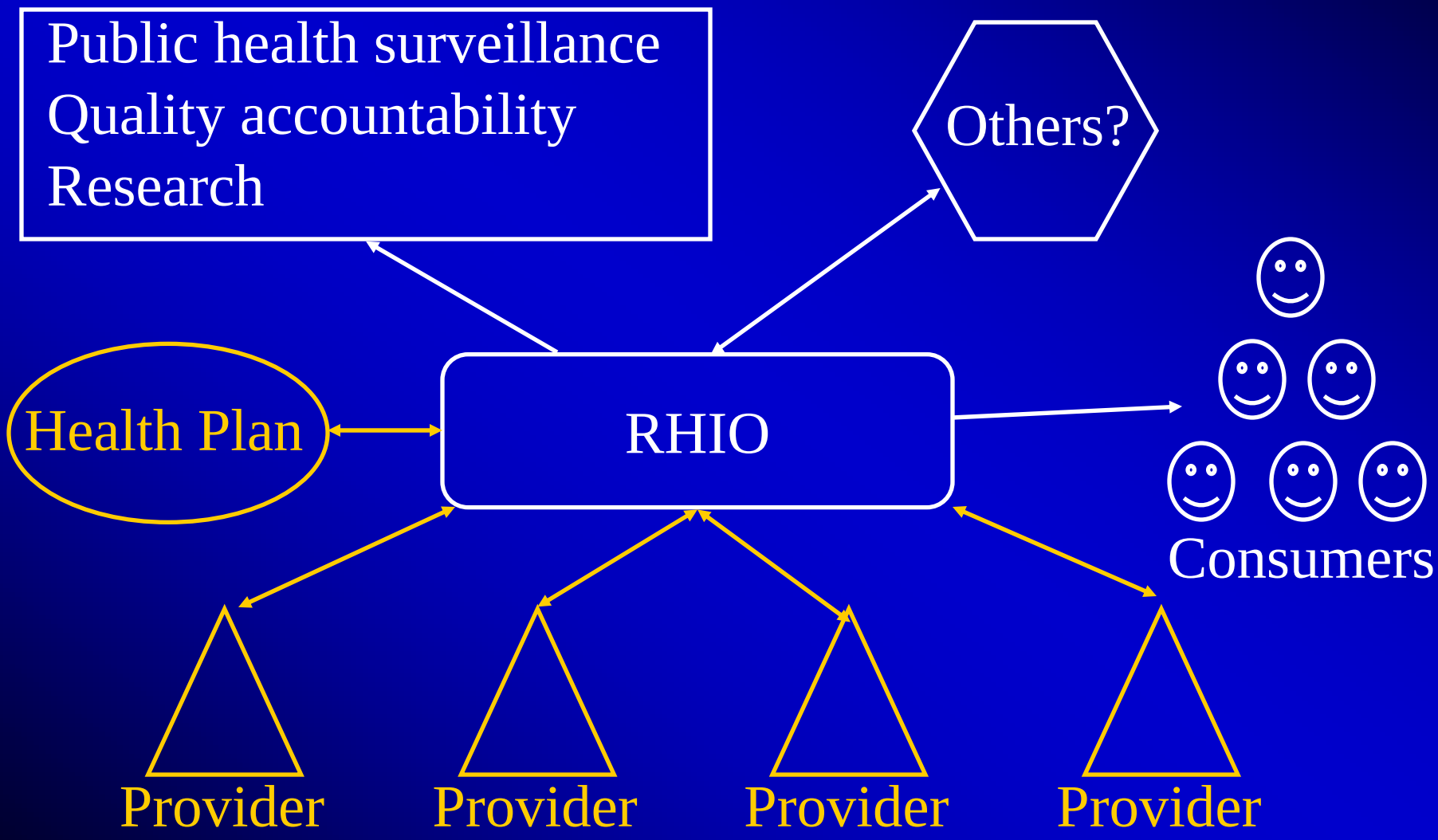
Goals of the NHII

- Improving population health
  - Unifying public health surveillance
  - Streamlining quality of care monitoring
  - Accelerating research and dissemination of evidence

Benefits for the Consumer

- Providers make better decisions, because--
  - They have better information
  - They use smart systems
- Improved public health surveillance and response
- Improved research and quicker adoption of best practices
- Consumers make better decisions because—
  - They have access to their own health information
  - They have qualitative information about providers

Regional Health Information Organization



Consumer Rights under HIPAA

- Is my information available on the network?
  - Will I know? Can I opt out? Can I keep sensitive information out?
- Who has access to my information on the network?
  - Will I know this? Can I control it?
- What uses can be made of my information on the network?
  - Will I know this? Can I control it?
- Do ***I*** have access to my information on the network? Can I change it?
- Will I find out about security breaches?
- Can I hold users accountable for misuse of my information?

Privacy under HIPAA

Will the network allow--

- Access by providers for—
  - payment
  - health care operations?
- Access by health plans for payment?
- Access by public health authorities?
- Access for research?
- Access by law enforcement authorities and private litigants?

Security under HIPAA

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

- To ensure confidentiality and integrity of information
- To protect against reasonably anticipated--
  - threats to security or integrity
  - unauthorized uses or disclosures

Security under HIPAA

- 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 and complexity
  - Technical infrastructure and capabilities
  - Potential risks to health information
  - Cost of security measures

Security under HIPAA

- Authentication – who is this?
- Authorization – what information can this user access?
- Logging and auditing
- Training
- Enforcement
- On-line access by medical staff

OMB's Electronic Authentication Guidelines

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

Policing the Exchange under HIPAA

- Not directly regulated
- Covered entities disclosing health information are required to obtain & enforce contractual assurances that the business associate 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 Exchange under HIPAA

- 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
- Covered entity has contract remedies only
- HHS has no direct jurisdiction
- No private right of action
- Consumer notification laws
- OIG security audits

The Electronic Health Record

ESIGN & UETA

- Allow retention of records in electronic form, as long as the records accurately reflect the information in the original, and remain accessible to all persons entitled to access.
- Allow signature requirements to be met by any electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.
- No digital signature requirement – yet.

The Electronic Health Record

- Transitioning to EHR
  - Retention of paper records
  - Hybrid records
  - Email
- Accuracy and authentication
- Alteration
- Retention
- Production and reproduction
  - Metadata and smart systems
- Transmission

Liability risks

- Privacy/security breaches
- Incomplete or inaccurate data
- Decision support systems
- The T. J. Hooper case