THE 13TH NATIONAL HIPAA SUMMIT

HEALTH INFORMATION PRIVACY & SECURITY IN SHARED HEALTH RECORD SYSTEMS

SEPTEMBER 26, 2006

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

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

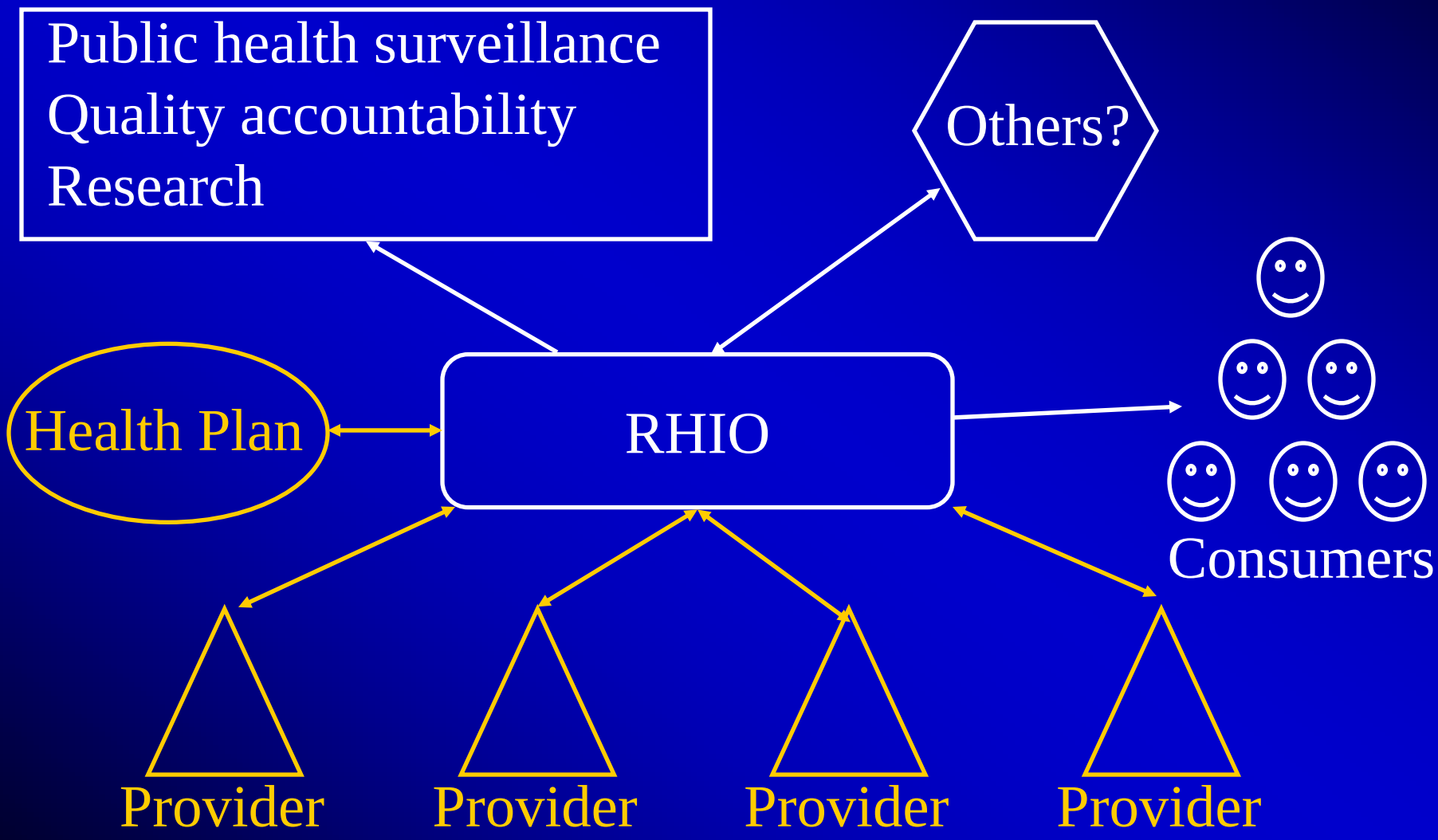
Goals of the NHII

- 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



What Am I Concerned About?

- Is my information available on the network?
  - Can I control this?
- Who is allowed 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?
- How secure is my health information on the network?
- What accountability is there for misuse of my information?

Consumer Rights under HIPAA

- HIPAA gives consumers rights to--
  - Access health information
  - Amend/annotate health information
  - Request restrictions on use and disclosure
  - Accounting of non-routine disclosures
  - Notice of privacy practices

Consumer Rights under HIPAA

- HIPAA does not give consumers rights to--
  - Decide whether to participate in electronic record exchange
  - Know whether information about them is being made available through an electronic exchange
  - Restrict what information is made available through the exchange, and to whom
  - Know who has had routine access to the information in the exchange
  - Get on-line access to information in the exchange
  - Receive notice of breaches of security of data in the exchange
  - Hold people accountable for misuses of data

Privacy under HIPAA

- All protected health information is the same
- Regulation of use and disclosure of health information is *permissive*, except
  - Disclosure to the individual
  - Disclosure to HHS for compliance
- Disclosure is generally permitted without consumer authorization for—
  - Treatment
  - Health care operations (including payment)
  - Public-interest related purposes

Privacy under HIPAA

Will the network allow--

- Access by providers for—
  - treatment
  - payment
  - health care operations
- Access by health plans for payment
- Access by public health authorities
- Access for research
- Access by law enforcement authorities
- Access by private litigants
- Access by social service agencies

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 in an Information Exchange

- Standards with implementation features, e.g.
  - Standard: access control
  - Implementation feature: Unique user identifier (password, PIN, biometric, etc.)
- Some implementation features are “addressable” (optional) – e.g., encryption

Security under HIPAA

- Authentication – who is this?
- Patient matching
- Authorization – what information can this user access?
- Logging and auditing
- Enforcement

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

- 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
- No private right of action