Securing the Health IT Ecosystem (laying track when the train is coming)

Presented by

Deborah Lafky , MSIS, Ph.D., CISSP
Office of the National Coordinator for Health Information Technology (ONC)
U.S. Department of Health and Human Services

TO: ISSA National Capital Chapter

June 15, 2010

The Imperative

From now on, our digital infrastructure — the networks and computers we depend on every day — will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority. We will ensure that these networks are secure, trustworthy and resilient.

President Barack Obama

May 29, 2009

The ONC Commitment

…We cannot achieve the benefits of a nationwide health information system unless we can assure all Americans that their personal health information will remain private and secure…Putting into place safeguards for the privacy and security of this information…will be an ongoing priority…

David Blumenthal, MD, MPP

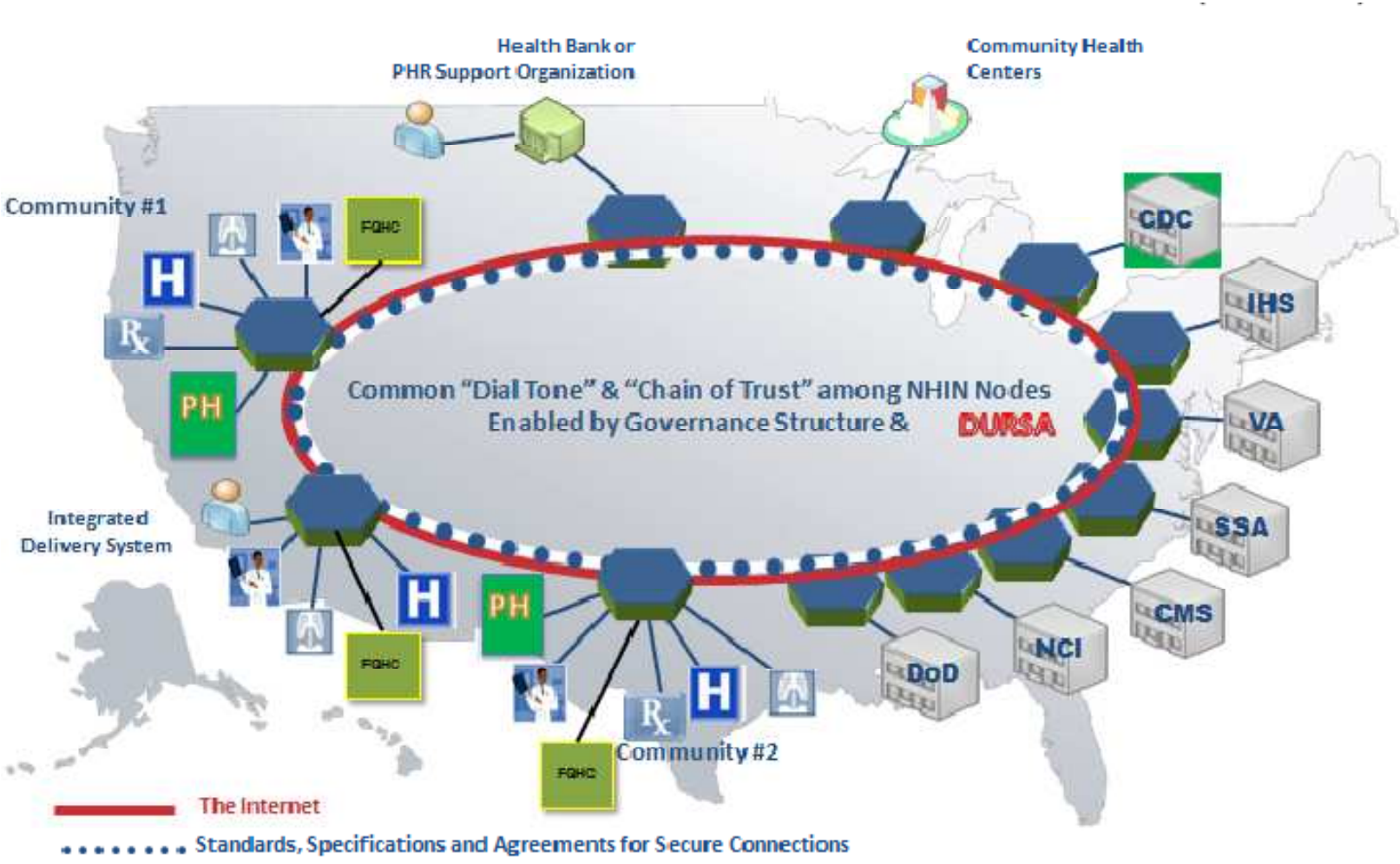
National Coordinator for Health Information Technology

August 20, 2009

Time is of the essence

What we hope to achieve

Inter-connected health information exchange across the nation



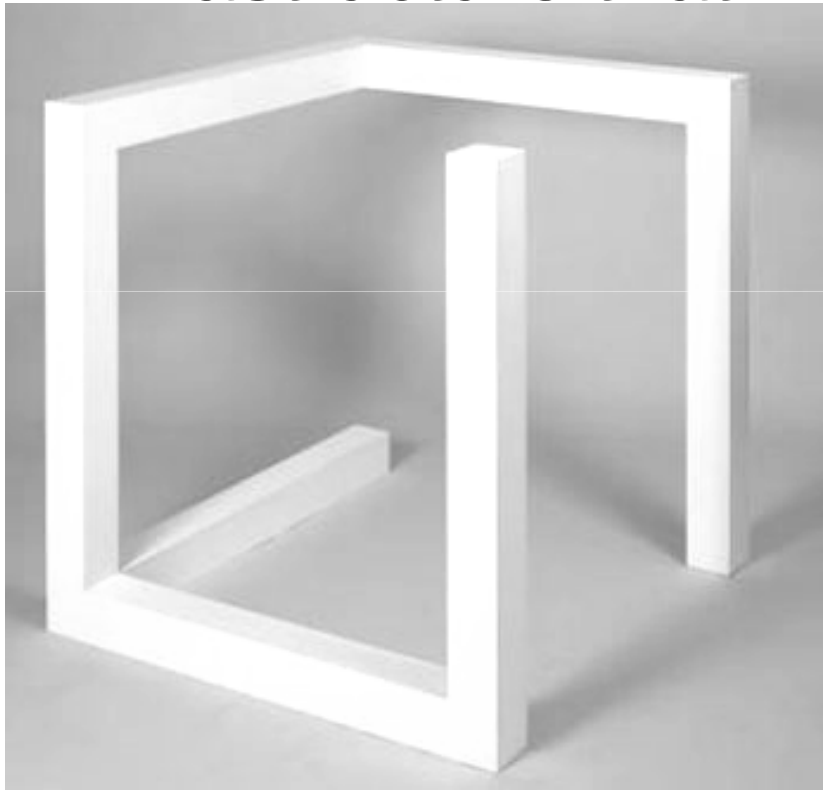
Where we are starting out from

A fragmented system marked by information islands and crossed channels.

The big challenge

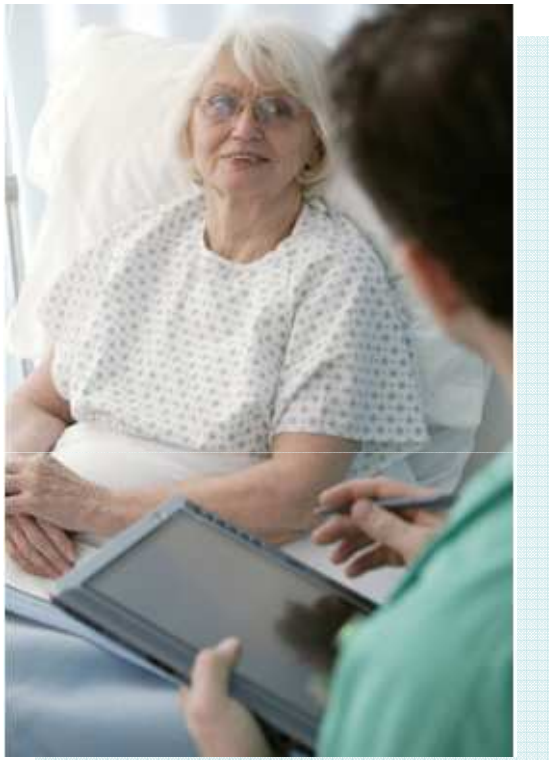
- How can we secure an infrastructure that is not yet built?

Or even completely designed?



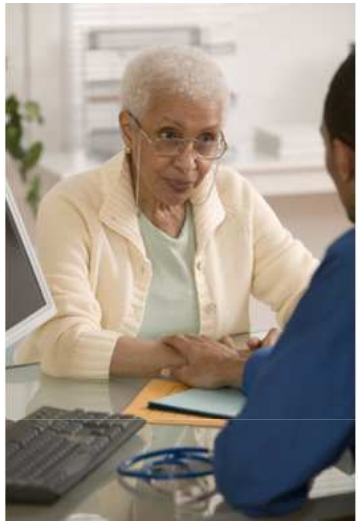
Nationwide health information exchange is still working out its architectural approach(es).

A Framework for Health IT Security and Privacy



Delivering Quality Health Care

- HIT is pivotal to modernizing health care and offers a number of benefits to patients and providers.
- Privacy and security are central to our HIT efforts.
- Efforts to develop policies and assess the levels of protection have been ongoing and basic laws are in place.
- ARRA/HITECH provides resources and imperative to align technology and policy as electronic health records roll out.
- ONC is leading these efforts in collaboration with other federal agencies.
- Progress continues and protections will continue to get better and better as the technology evolves.



Security Strategy: Prioritize High-Impact Projects

- Do what is infrastructure-independent
  - Security Strategic Planning
    - Risk assessment
    - Mitigation planning
  - Toolkit and methodology development
  - Education, outreach, and communications
  - Technology guidance

Current Security Projects

- Risk Assessment
- Capability Assessment
- Incident Response
  - Planning
  - Functional capability
  - Training
- Continuity of Operations
  - Planning
  - Functional capability
  - Training

Current Security Projects

- Education and Outreach
  - Regional Extension Centers
  - Health IT Resource Center (HITRC)
  - Workforce Development
    - Community college
    - University-based
  - HIT Privacy and Security “landing page”
- NHIN Exchange and NHIN Direct
  - Designing for security and privacy
  - Data use agreements

Use Government Levers

- Regulations
  - EHR Certification and Standards
    - Access Control
    - Audit
    - Authentication
    - Integrity
    - Transmission security
    - Infrastructure
  - Increased accounting for disclosures
  - Breach notification

Use Government Levers

- Incentives
  - Meaningful Use
    - Rewards adoption of electronic health records, but only if they are certified — certification criteria include security