



HIMSS Public Policy Forum

Health IT Priorities in the New Political Landscape

October 28, 2008

Jodi G. Daniel, J.D., M.P.H.

Director, Office of Policy and Research
Office of the National Coordinator
for Health Information Technology
U.S. Department of Health and Human Services



Agenda

- ONC Background
- Current Privacy and Security Policy Environment
- Policy Challenges and Opportunities



ONC Background

- 2004 – Executive Order 13335
 - Established the position of National Coordinator for Health IT
- 2004 – Framework for Strategic Action
- 2006 – Executive Order 13410
 - Health IT; Quality Information; Price Information; Quality and Efficiency of Care
- 2008 – The ONC-Coordinated Federal Health IT Strategic Plan: 2008-2012

Goals, Objectives, and Strategies

- Two goals:
 - Enable patient focused health care
 - Improve population health
- Four objectives for each goal:
 - Privacy and Security; Interoperability; Adoption; Collaborative Governance
- Numerous strategies and milestones for each objective

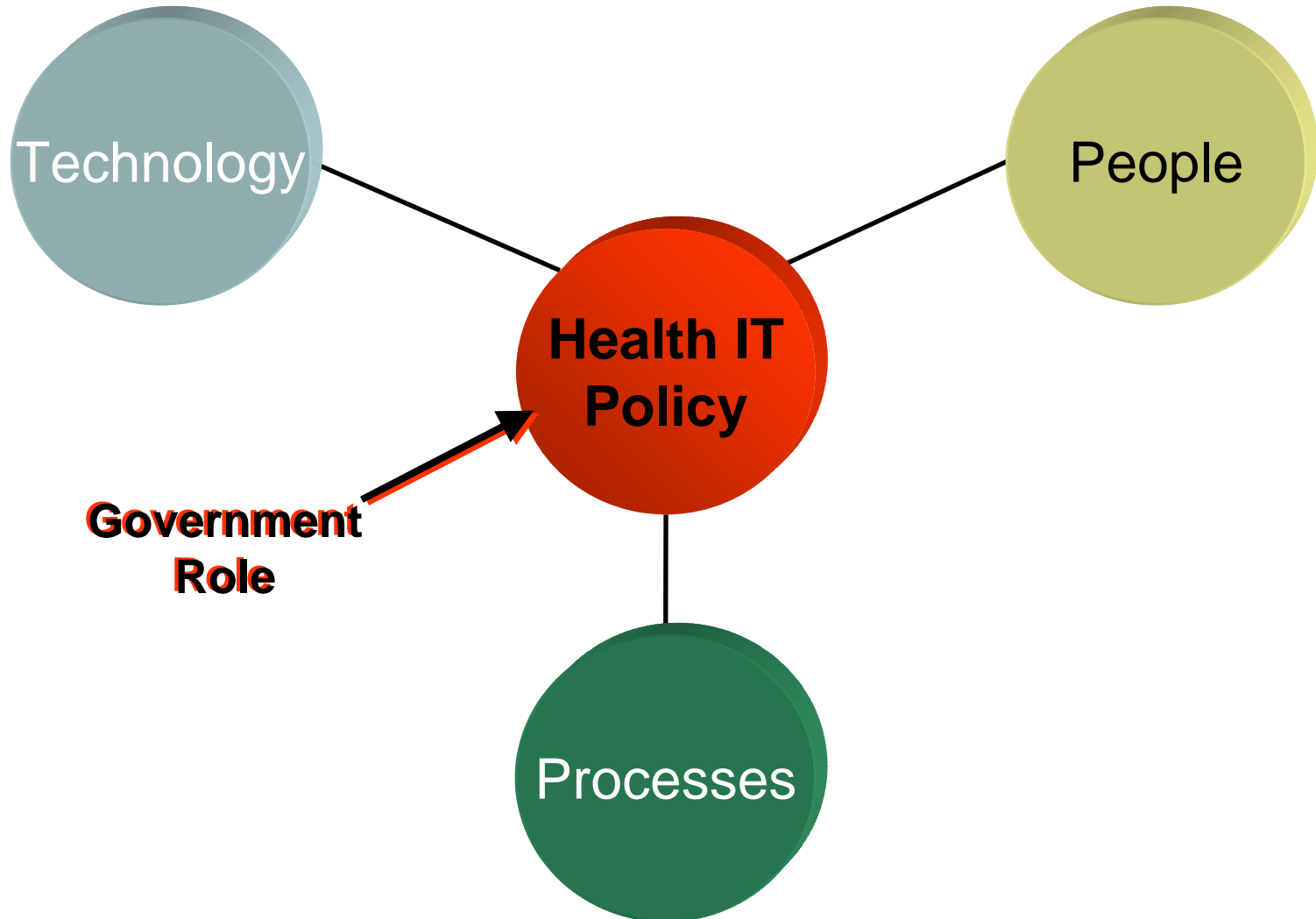
Robust privacy and security protections will be the underpinning of a successful network for health information exchange.

*– HHS Secretary Michael Leavitt,
HIMSS 2008 Keynote Address*

Privacy and Security Strategies

- Develop a privacy and security framework
- Continue to work at the state-level
- Identify best practices (technology & policy)
- Increase stakeholder understanding
- Identify and evaluate approaches to better coordinate Federal policies

Where Does Health IT Policy Fit?



Current Privacy and Security Policy Environment

- 1970s - Confidentiality of Alcohol & Drug Abuse Patient Records regulation
- 1974 - Privacy Act
- 1996 - Health Insurance Portability and Accountability Act (HIPAA)
 - HIPAA Privacy and Security Rules
- 2002 - Federal Information Security Management Act (FISMA)
- 2008 - Genetic Information Nondiscrimination Act (GINA)



Tension Between Access and Protection

Access

- Greater consumer involvement in health care
- Improved care coordination
- Increased quality
- Added convenience



Protection

- Increased trust
- Increased participation

Policy Spectrum: Who Controls?

United States

European Union



Data Holder Centric

- *Those who hold data must follow rules to protect the data and how data can be used.*

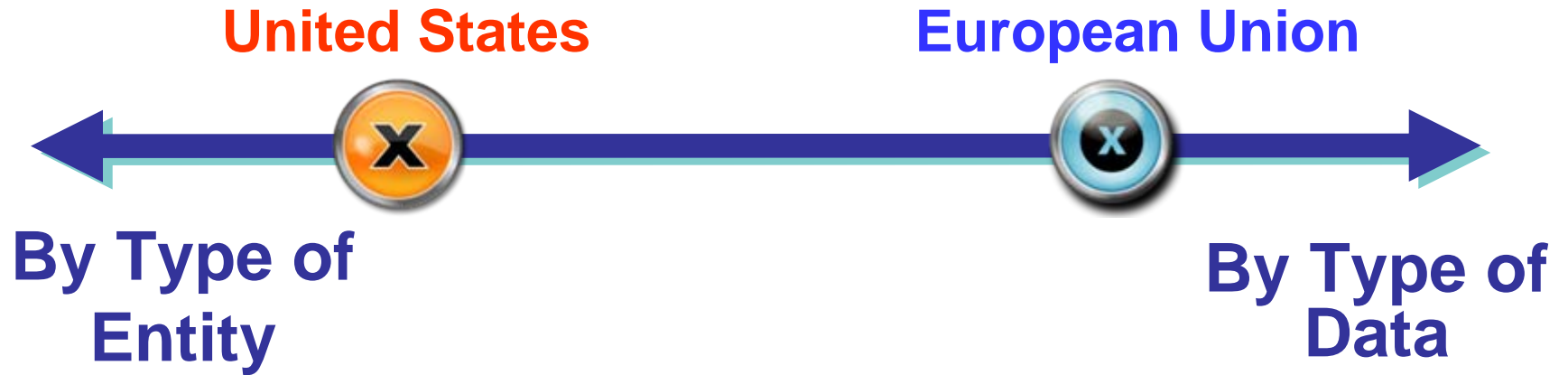
Combined Approach

- *Combination of consumer control and rules for how data users can act.*

Consumer Centric

- *Consumer determines who has access to data and for what purpose.*

Policy Spectrum: Approach to Protections



What can the Federal Government Do?

- Accreditation/Certification
- Bully Pulpit
- Procurement
- Incentives/Disincentives
- Legislation
- Regulation
- Adopt policies in programs



Policy Challenges and Opportunities

Focus for the future:

Revisit Prior
Policies? or

Consider New
Issues?

What's New?

- Capabilities to link data
- Capabilities to look up patient information
- Opportunities for enhanced protections
- Opportunities for greater consumer involvement
- Opportunities for increased consumer electronic access to their information

Issues: Who Should Comply with Protections?

- Only covered entities?
- Non-covered health care providers?
- Health information organizations (HIOs)?
- Service providers?
- Health record banks?
- Others that may connect to a health care network?
- Others that may receive health information?

Issues: What Information for What Purposes?

- What Information?
 - Only networked health information or all information?
 - Only identifiable information? De-identified info?
 - How does minimum necessary work in a networked environment?
- What Purposes?
 - Should purposes of network access be limited?
 - All purposes under HIPAA?
 - Limited purposes?
 - Secondary uses of information?

What are the Right Level of Protections?

- New opportunities for greater protections through health information exchange?
 - Greater consumer permissions?
 - Greater consumer access?
 - More limits on access by others to information?
 - Consumer-oriented audit logs?
 - Flags to detect aberrant activity

Other Policy Issues

- Different standards for networked information?
How is the line drawn?
- Verification of identity and authority in networked environment
- How are protections defined, applied, enforced?
- Breach notification?
- How are errors addressed?

Considerations for Policy Development

- Recognize the foundation of privacy protections at a state and federal level
- Prevent unintended consequences:
 - Use policy mechanisms that can adapt with technology changes
 - Consider impact on patient care
- Build consensus through stakeholder involvement
- Prioritize



For More Information

<http://www.hhs.gov/healthit>