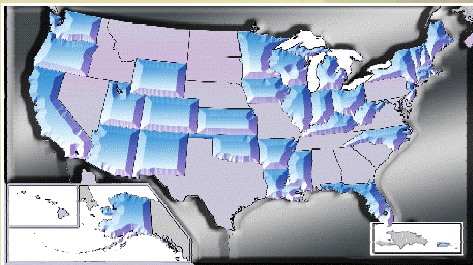


Health Information Security and Privacy Collaborative

Regional Meeting

October 25, 2006 - Minneapolis, MN

Advancing State Approaches Towards Solutions and Implementation



Walter G. Suarez, MD, MPH
Institute for HIPAA/HIT Education and Research

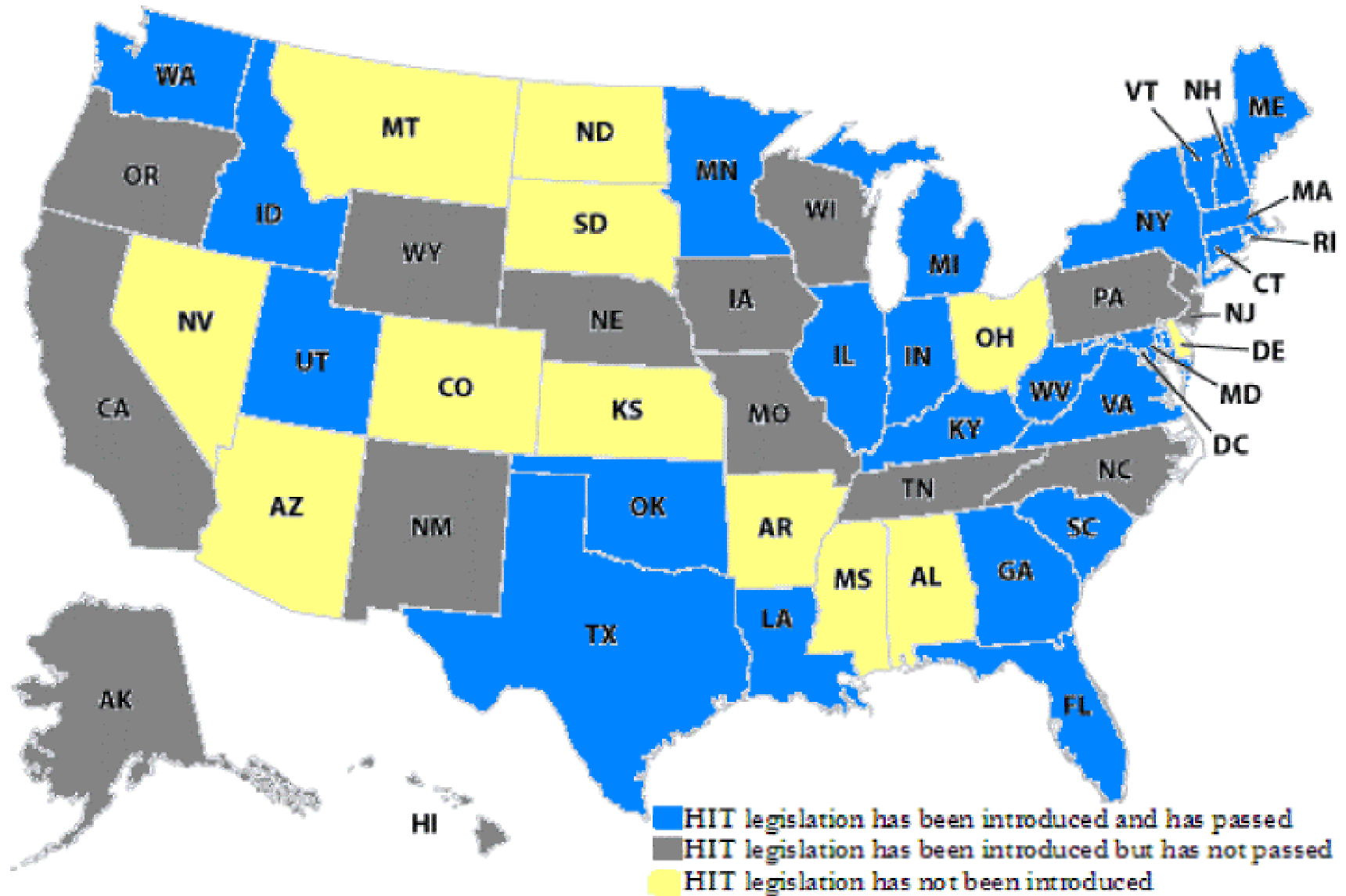
Introduction

- Since HIPAA implementation started in 2003, a new set of national, regional, state and local initiatives have emerged
- Focus: Adoption of interoperable health information technology infrastructure
- New Vocabulary and Terminology:
 - HIE, HIT, EHRs, PHRs, RHIOs, NHIN
 - AHIC, HISTP, HISPC, CCHIT

Introduction

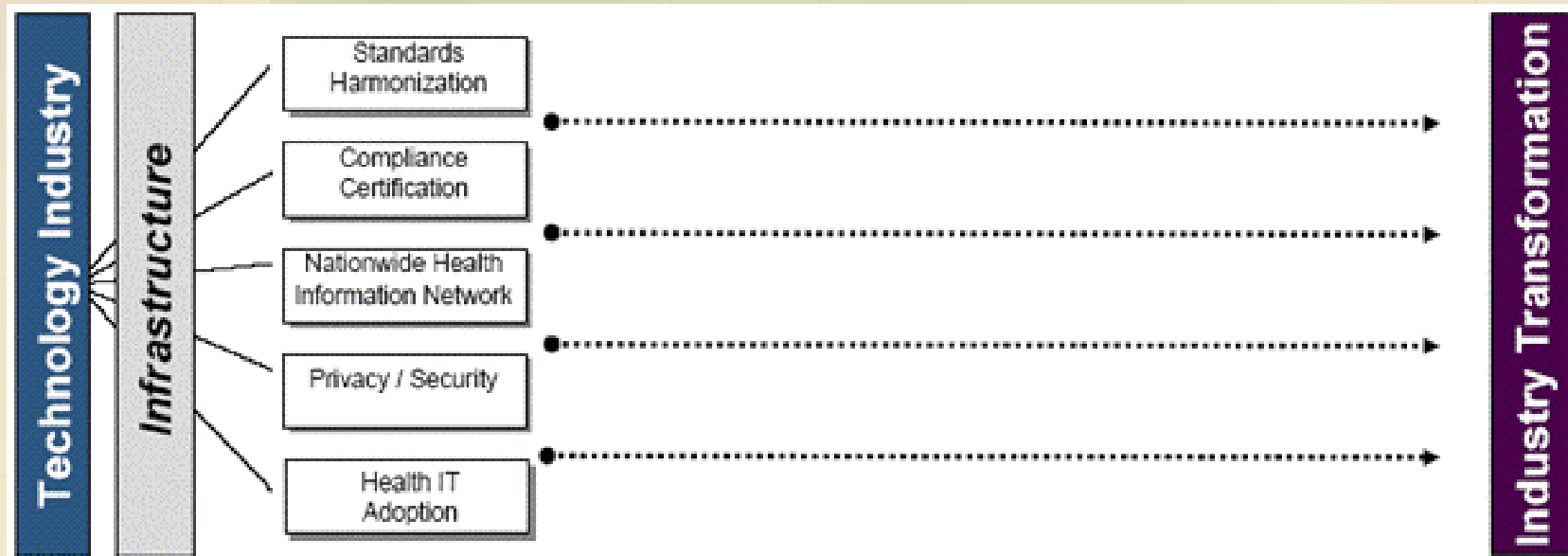
- Privacy and Security
 - Critical component in all emerging national, regional and local HIE efforts
 - Revisited from the earlier “HIPAA Days” with a new perspective and new areas of applicability
 - Not just administrative transactions
 - Current and emerging electronic health information exchanges of clinical data

State Legislative Activity in 2005 and 2006 - State by State Analysis

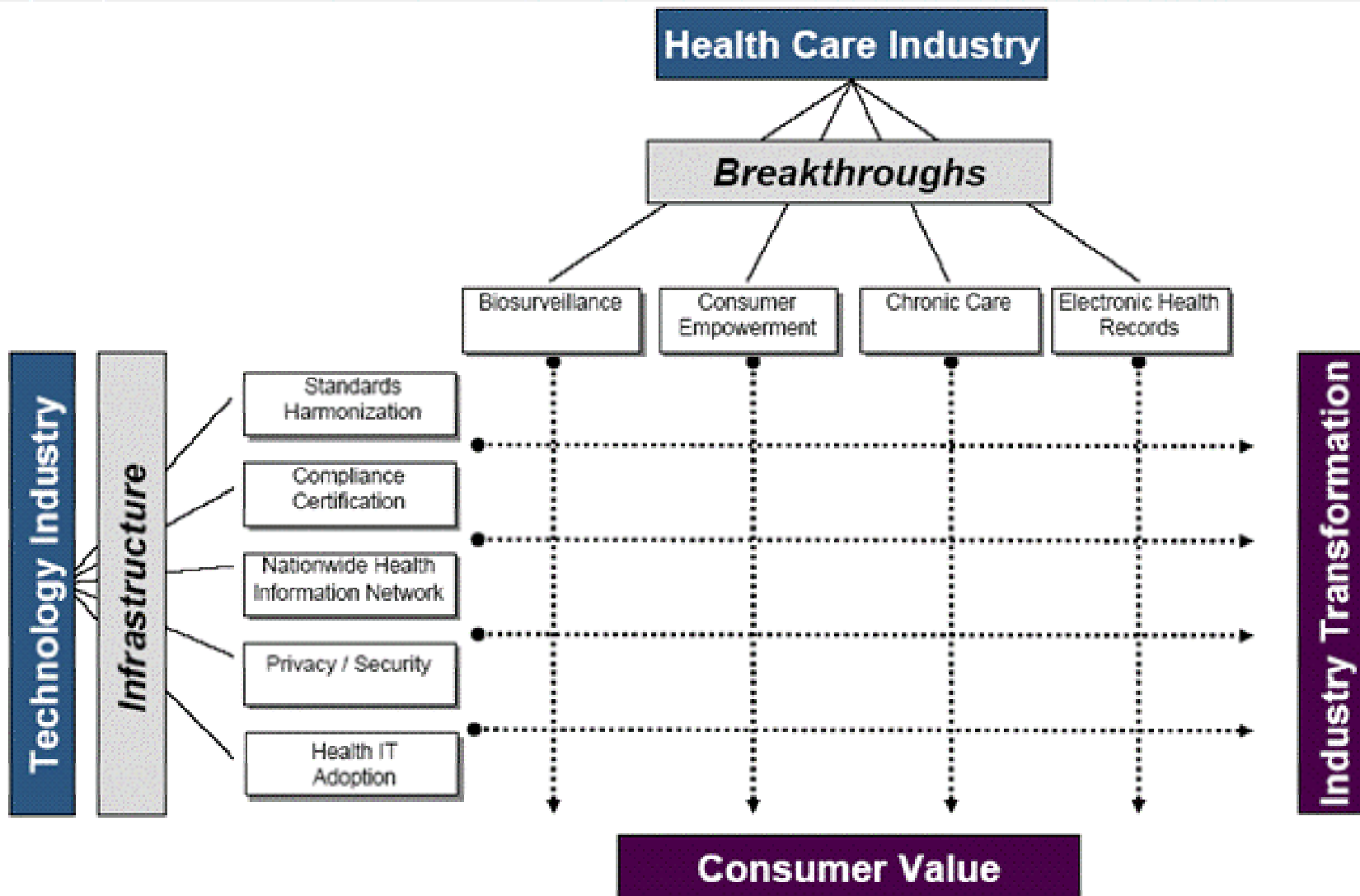


Source: Third Annual Survey of HIE Activities at State, Regional and Local Levels. eHealth Initiative, September, 2006

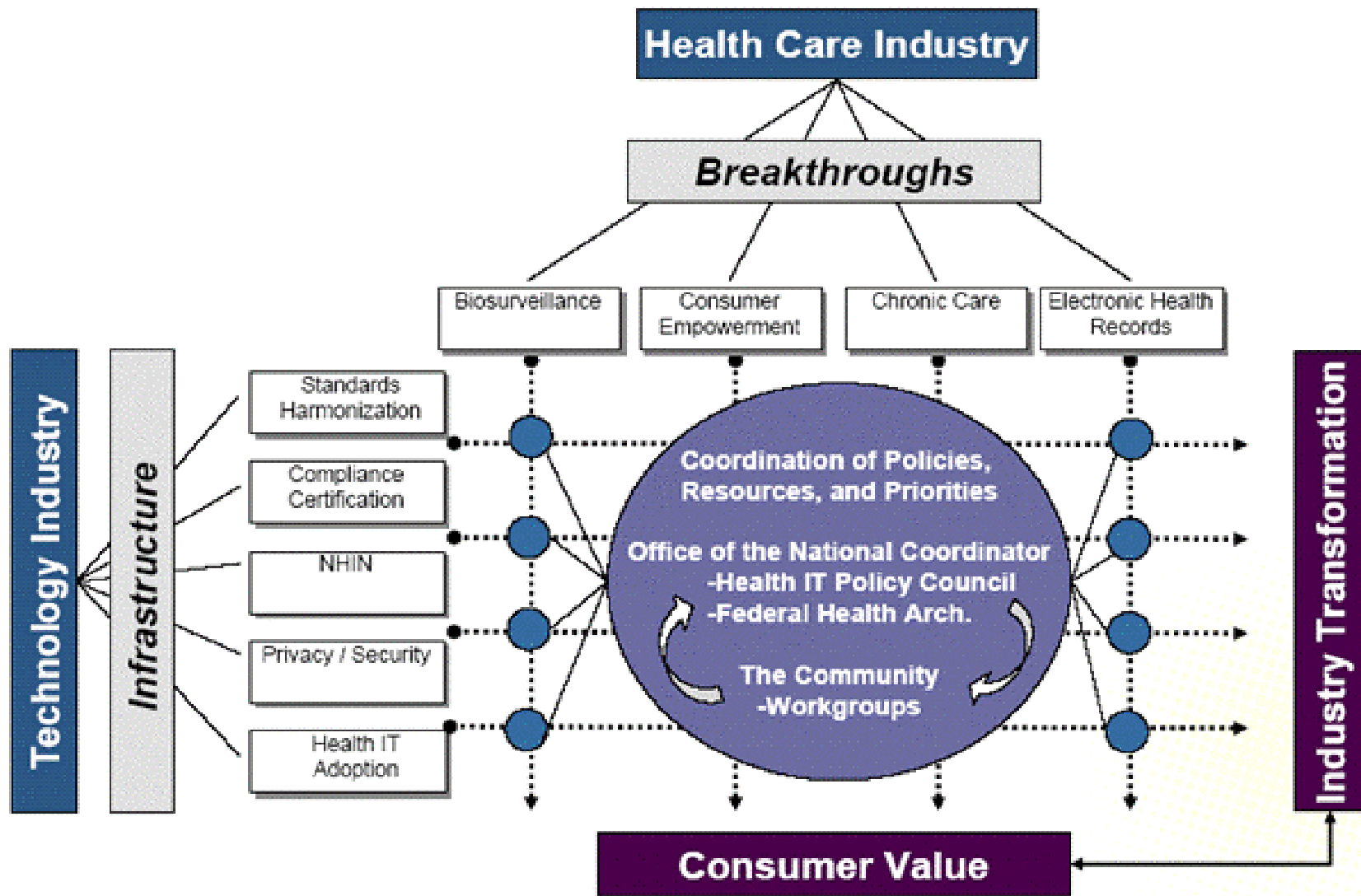
The National Health IT Strategy



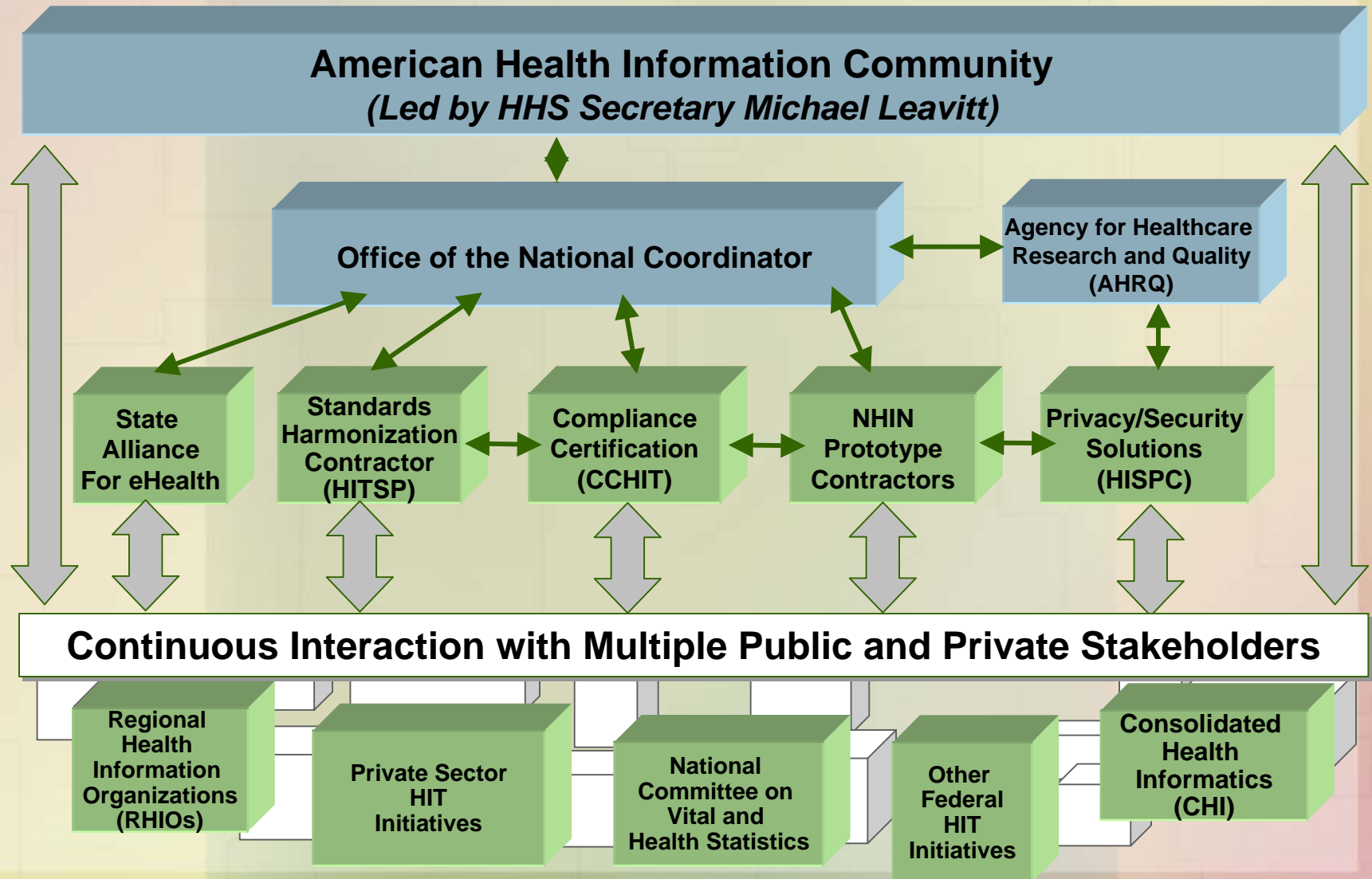
The National Health IT Strategy



The National Health IT Strategy



The National Health IT Strategy



National HIT Efforts:

Privacy and Security Implications

- AHIC – Privacy, Confidentiality and Security Workgroup
 - Charge:
 - Make recommendations to AHIC regarding the protection of personal health information in order to secure trust and support appropriate interoperable electronic HIE
 - Make actionable confidentiality, privacy and security recommendation on specific policies that best balance the needs between appropriate protections and access to health information

National HIT Efforts:

Privacy and Security Implications

- AHIC – Privacy, Confidentiality and Security Workgroup
 - Areas of work include (but are not limited to):
 - Methods of Patient Identification
 - Methods of Authentication
 - Mechanisms to Ensure Data Integrity
 - Methods for Controlling Access to Personal Health Information
 - Policies for breaches of Personal HI confidentiality
 - Guidelines and processes for appropriate secondary uses of data
 - Scope of work for a long-term independent advisory body on privacy and security policies

National HIT Efforts:

Privacy and Security Implications

- **Certification Commission for Health Information Technology (CCHIT)**
 - Recognized independent, voluntary certification authority for electronic health records and their networks
 - Comprehensive product evaluation criteria:
 - **Functionality** – setting features and functions to meet a basic set of requirements
 - **Interoperability** – enabling standards-based HIE with other sources of healthcare information
 - **Security** – ensuring data privacy and robustness to prevent data loss



National HIT Efforts:

Privacy and Security Implications

- Certification Commission for Health Information Technology (CCHIT)
 - Priorities:
 - Ambulatory EHR Products (2006)
 - Inpatient EHR Products (2007)
 - Network Certification (2008)
 - Type or Security Criteria/Domain Categories
 - Authentication
 - Audit
 - Access Control
 - Back-up/Recovery
 - Documentation
 - Security and Reliability
 - Technical Services

National HIT Efforts:

Privacy and Security Implications

- Health Information Technology Standards Panel (HITSP)
 - Leading standards harmonization process
 - Delivered to ONC first set of harmonized standards on three used cases
 - Biosurveillance
 - Electronic Health Records
 - Consumer Empowerment
 - Standards focus on transmission messages (data content and format)
 - Security standards not currently covered

National HIT Efforts:

Privacy and Security Implications

- Nationwide Health Information Network (NHIN)
 - Four consortia developing prototypes in local/regional markets
 - Considering basic architecture elements, functional requirements, services that could be offered by a HIN service provider
 - Privacy and security a major component

National HIT Efforts:

Privacy and Security Implications

- Nationwide Health Information Network (NHIN)
 - Second NHIN Forum (September, 2006) focused on HIN Security and Services
 - Emerging Issues (Security)
 - Identity Management Issues
 - Patient, Provider, User Identification and Authentication
 - Patient-driven Authorization and Access Controls
 - Auditing Data Access
 - Confidentiality and Secondary Uses of Data

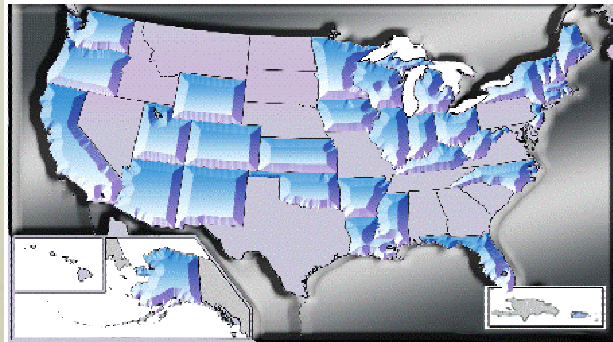
National HIT Efforts:

Privacy and Security Implications

- National Committee on Vital and Health Statistics (NCVHS)
 - High Level Functional Requirements for a NHIN
 - Applicable to (external) exchange of health information between entities in a region or within the NHIN
 - Consistent with NHIN prototype applications and national/regional discussions

NCVHS High Level Functional Requirements for NHIN

- 1. Certification**
- 2. Authentication**
- 3. Authorization**
- 4. Person Identification**
- 5. Location of Health Information**
- 6. Transport and Content Standards**
- 7. Data Transactions**
- 8. Auditing and Logging**
- 9. Time-sensitive Data Access**
- 10. Communications**
- 11. Data Storage**



**Health Information Security and Privacy
Collaborative (HISPC)**

Review of State Findings

Considerations for Identifying and Documenting Solutions

- **General context for the proposed solution**
- **What is the proposed solution**
- **What domains the solution addresses**
- **What types of health information exchanges are being addressed with the solution**
- **Which stakeholders will be primarily affected/involved**
- **What HIE barriers will the solution address**
- **Stage of development of the proposed solution and extent to which proposed solution is in use**
- **Extent to which solution might be appropriate for a wide range of stakeholders and HIEs**
- **Possible barriers to solution (including legal, technical, cost, etc)**