California eHealth Collaborative Webinar: May 17, 2011

State of California Office of Health Information Integrity (CalOHII)

CalOHII Demonstration Projects for the Electronic Exchange of Health Information

Assembly Bill 278

[Health and Safety Code 130275 et seq.]

- Establish and administer demonstration projects
- Adopt regulations
- Report results to the Legislature

Context of AB 278

- The American Recovery and Reinvestment Act of 2009 (ARRA)
- Office of the National Coordinator (ONC) awards California a four year program grant totaling 38.8 million dollars, beginning in fiscal year 2009-2010
- CalPSAB work on privacy and security

Lessons learned in HISPC

- Both state and federal law currently regulate medical and health privacy and security requirements
- The HIE capabilities raise new consumer privacy and provider liability concerns not addressed or envisioned in existing laws
- Failure to effectively address these critical concerns would lead to poor consumer and provider participation into newly created systems.

CalOHII

- HIPAA interpretations & guidance for Governmental entities
- Oversee federal grant and CEC development of HIE infrastructure
- Sanctions for unauthorized access into medical information
- CalPSAB & HISPC

CalOHII to meet federal grant requirements:

- CHHS grant proposal relied on CalPSAB work
- Leadership role and responsibility for law harmonization and framework for privacy and security
- Demonstration projects is one of many tools being used

CalPSAB

Early supporter for demonstration projects

- Costs
- Implementation strategies
- Transparency of data flows

CalPSAB established in October 2007

MISSION STATEMENT –

Develop and recommend privacy and security policies for California Health Information Exchange (HIE) that promote quality of care, respect the privacy and security of personal health information, and enhance trust.

PSAB Membership

Members appointed by secretary from Health Care Associations representing:

- Private providers
- Private payers
- Other private industry representatives
- Consumers
- Government members
- Education members
- Vendors

CalPSAB early work

- HIE Principles
- Data Flows
- Adequacy of de-identification
- Concerns on secondary uses
- Baselines for privacy and security

CalPSAB Guidelines

- July 2009
- List serve 425 to 491
- 29 meetings
- 14 Survey Monkeys—207 responses
- Public comments: 33 organizations & 1,232 individuals responded

Consent

- 2008- no consent, opt-out & opt-in
- September 2009: Bi-furcated
- December 2009: withdrawn
- Task group meetings
- June 2010: split decision
- October 2010: consensus

Security Guidelines

- Objectives
- Principles
- Process
- Sources
- People

Security Committee Objectives

- Adopt security standards promulgated by Standards Development Organizations (SDOs) for electronic health information exchange.
- Identify security standards gaps for California not addressed by federal standards.
- Develop implementation strategy for the approved solutions.

Security Committee Deliverable

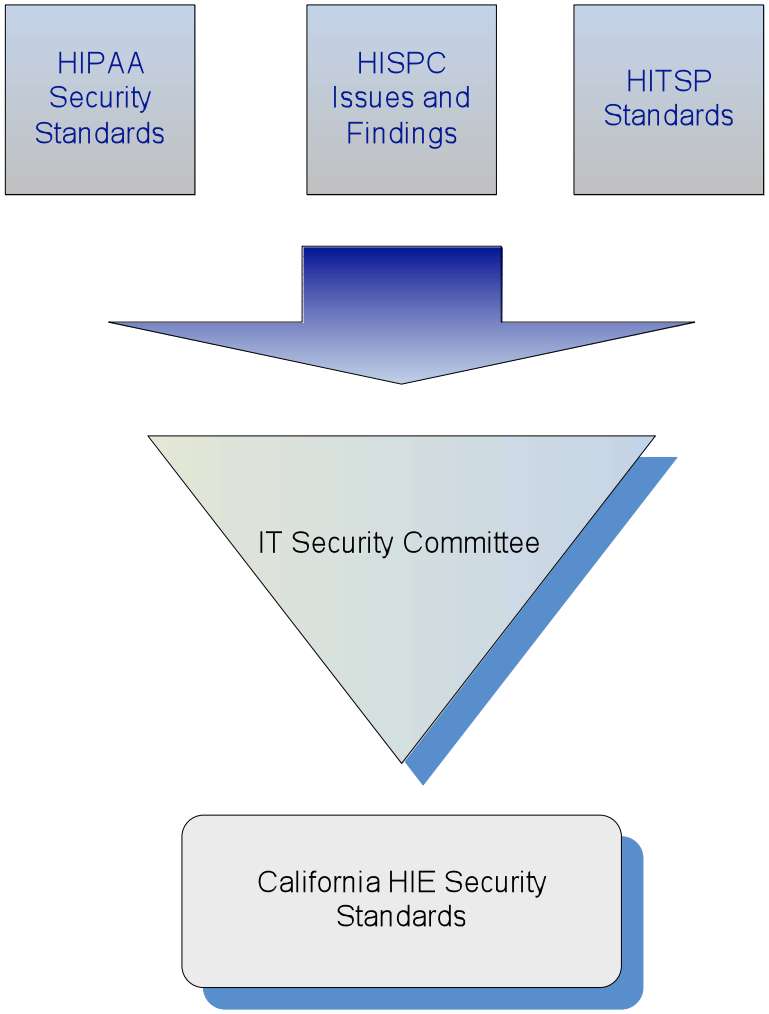
Original charter for the PSAB Security Committee:

Recommend security standards for California to the Privacy & Security Advisory Board to be promulgated by the California Health and Human Services Agency Secretary.

Principles of Standards Adoption

- Adopt California's security standards upon existing international standards, national standards, federal law, national workgroup standards, FIPS, NIST, ISO, other state's standards, local RHIO standards, etc.
- Utilize subject matter expertise from California's public, private, and community institutions in the selection of each standard and development of each reference implementation.

Security Committee Process



- Determine a base for security standards
- Evaluate security issues identified as barriers in HISPC
- Evaluate security standards promulgated by HITSP
- Evaluate security standards and best practices in the Health IT industry

Process

- When evaluating security standards for adoption we need to keep in mind:
  - Cost of implementing the security standards
  - Level of protection security standards provide
  - How the standard will assure protection of health information for consumers
  - Solicit feedback from small providers and consumers
- NOTE: While its foreseeable that there will be a floor of security requirements, like HIPAA, organization size & complexity will dictate additional controls.

Started with an Environmental Scan

- HIPAA (1996; regs 2001-2003)
- ISO 17799 (2005) – now is 27002 (2007)
- COBIT 4.0 (1996, 2007)
- SOX (2002)
- PCI DSS (2006)
- GLBA (1999)
- PIPEDA (Canadian) (2000)
- NIST (SP-800) (several)
- CA-OCIO (2007-8)
- HITSP (2007-8)

Baseline Standards Domains

Administrative Controls

- Information Security Organization & Responsibility
- Risk Assessment & Treatment
- Security Awareness, Education & Training
- Workforce Security & Incident Management
- Compliance Testing, Audit & Monitoring
- Contracts & Agreements

Business Continuity & Contingency Planning

- Business Continuity
- Contingency Planning
- Testing and Revision

Facility & Equipment Controls

- Facility Access Controls
- Device and Media Controls
- Technical Controls

Data Protection and User Access Controls

- Authentication & Authorization (Access Controls)
- Data Assurance

Access Control

- Authentication (Ca OCIO Proposed Std.)

  Authentication performed through a combination of direct, trusted third party, and federated chain of trust relationships based on WS-Security.

- Authorization (NIST 800-95, ABAC)
  - Data Source
  - Entity of Requestor
  - Role of Requestor
  - Consent Directives of the Data Subject
  - Use of Data
  - Sensitivity of Data
  - Form / Method of Use

- Identity Management (Ca OCIO + NIST)

  Federated with proofing and provision for establishment and revocation of privilege delegation

- Session Controls

  Not yet addressed

Security Committee Composition

- 7 counties,
- 21 provider entities,
- 5 health industry-related companies,
- 9 state departments,
- 2 health information exchanges, and
- 5 health industry associations.

Members are mostly security professionals – many CISOs and many with CISSP credentials

CalOHII Demonstration Projects

Establish and administer demonstration projects for the electronic exchange of health information

- Up to four demonstration projects each year
  - Two selected as the first participants

CalOHII Demonstration Projects

- Adopt regulations
  - Proposed regulations posted for public comment March 1, 2011
  - Over one hundred comments received from stakeholders
  - CalOHII is drafting responses to the comments
  - CalOHII is drafting revisions to the proposed regulations
  - Aiming to post the regulations for another round of public comments by end of May

CalOHII Demonstration Projects

- Regulations – the process
  - 30 day comment period
  - Public hearing
  - Submit to Office of Administrative Law
  - File with the Secretary of State
  - Publication in the California Code of Regulations

Demonstration projects are just one of many tools CalOHII is using:

- Security Committee
- Privacy Committee
- Enforcement
- CeC infrastructure development
- HIE Coordinator

QUESTIONS?