Beyond FISMA – a Policy Framework for an Interconnected World

Information Security and Privacy Board Meeting
July 14, 2011

Julie Boughn
Ryan Brewer
Ms. Ashley Corbin

Centers for Medicare & Medicaid Services (CMS); Director, Division of Research, Innovation and Standards

Henry Chao
Health Care Environment Drivers

• Health Information Exchange/Interconnectivity
  o Moving from small scale trials and pilots to operations
  o The dilemma of boundaries and data ownership
• Open Government/Transparency Initiative
• Increasingly diverse set of partners and stakeholders
  o Undefined expectations around appropriate security posture to conduct business
Health Care Environment Drivers

Security Concerns

• Shifting boundaries/parameters around shared Federal healthcare data without clear delineation of ownership and related security responsibilities
• Increased dynamic inbound/outbound movement of data across federal and non-federal partner boundaries
• Higher degree of data blending coming from different sources impacting traceability, accountability and ownership
• Existing trust partnerships have been traditionally built to apply in a one-to-one model, shifting to one-to-many or many-to-many
Security Considerations for Adoption of a Widespread Health Information Exchange Model

- Based upon applicable law and broadly construed existing frameworks
  - For Federal entities – FISMA
  - For non-Federal entities that are Covered Entities and Business Associates – HIPAA
  - Other laws or frameworks – Privacy Act, ITIL, ISO/IEC 27001, COBIT

- Parties to an exchange may also seek compliance with a variety of additional expectations and desire to establish formal mechanisms based around trust

- Uniformity and compatibility will be essential for nationwide exchange of health information
Policy Considerations

• Federal agencies currently have different expectations for “appropriate security” of non-Federal interfaces
• This creates complexity and burden for non-Federal entities that wish to exchange information with multiple Federal agencies
• Consistent definitions and expectations around appropriate security of interfaces would:
  o Further health care interconnectivity to support national initiatives
  o Address complexity and confusion
  o Provide flexible options to meet the needs of varied health care operations
  o Provide direction that is independent of scale

Longer-term, there is a need for a consistent nationwide information security posture for all interconnected health care stakeholders
## Trends in National Health Care Initiatives

<table>
<thead>
<tr>
<th>TRENDS</th>
<th>TOPICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Up Arrow]</td>
<td>HIT Exchanges as the primary path to meet National Health Care agenda (Meaningful Use, Health Insurance Exchanges, ACOs)</td>
</tr>
<tr>
<td>![Green Up Arrow]</td>
<td>Organizations that are, or will potentially participate in a health care exchange model (federal and non-federal) placing infrastructure, applications and data in cloud hosting environments</td>
</tr>
</tbody>
</table>

### Positive Drivers
- ONC has established centrifugal force and the health care industry has remained engaged
- Federal Government has championed the “Cloud First” initiative and they have also taken steps to address Cloud Computing security concerns via FedRAMP

<table>
<thead>
<tr>
<th>TRENDS</th>
<th>TOPICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Red Down Arrow]</td>
<td>Number of National Health Care initiatives that place a focus on ensuring that security and privacy are critical components of expanded health care interconnectivity</td>
</tr>
<tr>
<td>![Red Down Arrow]</td>
<td>Availability of national level, prescriptive direction around the definition of acceptable security and privacy controls and common security frameworks in Health Care interconnectivity</td>
</tr>
</tbody>
</table>
Harmonized Security and Privacy Framework for ACA Exchange Program

Challenges and Approach

July 14, 2011
Agenda

- Background (Patient Protection and Affordable Care Act)
- Security Challenges
- Pragmatic Approach for Adoption of Framework
- Harmonized Security and Privacy Framework
- Questions
States will implement / operate an Exchange, or HHS will do so on behalf of a state.

Under the Act, each state has a health insurance Exchange:

- Organized marketplace to
- Help consumers and small businesses
- Buy health insurance with
- Easy comparison of available plan options:
  - Price, benefits and services, and quality
Information Security: Balancing Issues and Challenges

Governance and Authority

- Balance FISMA, HIPAA, HITECH, Privacy Act, and state laws against ACA requirements
- Follow 26 USC §6103, Safeguards for Protecting Federal Tax Returns and Return Information (and related provisions)

Numerous Security Frameworks, Audits, and Certifications

- CSA
- NIST SP-800
- ITIL
- HIPAA
- CAG
- State Frameworks
- OCTAVE
- ISO2700
- CMMI
- ISO2702
- CSI
- COBIT
- PCI
- CSF

Resource Demands

Multiple assessments via different frameworks is expensive – measures but does not improve security

Threats

- CSA
- NIST SP-800
- ITIL
- HIPAA
- CAG
- State Frameworks
- OCTAVE
- ISO2700
- CMMI
- ISO2702
- CSI
- COBIT
- PCI
- CSF
Common goal of state and federal Exchange programs: maintain confidentiality and integrity of systems and data

Must consider wide variance among each service provider:
- Capabilities
- Resources
- Strategies
- Policies
- Standards
- Physical security
Our aim: Build a pragmatic approach to security for wide adoption

- Leverage
  - Existing bodies of work
  - Resources
  - Lessons learned

- Reduce
  - Burdens of security
  - Assessments

Enforcement protocol for interaction with Exchange IT solutions should encourage commitment to invest in enforcement of IT security principles
CMS has written a draft titled “Harmonized Security and Privacy Framework – Exchange Technical Reference Architecture (TRA) Supplement”

- **Goals:**
  
  Foster a collaborative discussion on security and privacy between the states and CMS

  Assure that the overall Exchange solution provides **necessary, effective security and privacy** for the respective systems and data in **compliance with all applicable federal and state security and privacy laws** and regulations

CMS will evolve the Harmonized Security and Privacy Framework in collaboration with the states
Harmonized Security and Privacy Framework

Key Topics in the Draft Supplement

- System and Data Classification
- Security Controls
- Identity, Credential, and Access Management
- Secure Infrastructure and Cloud Computing
- Data Encryption
- Auditing
- Continuity of Operations and Disaster Recovery
- Compliance Oversight
- Privacy Consideration
Harmonized Security and Privacy Framework
Three Phases for Development

Phase 1: Guidance on most important security and privacy considerations to establish a harmonized framework for the Exchange Architecture

Phase 2: Baseline definition and requirements to guide implementation

Phase 3: Detail to enable compliant operations and oversight
Desired Outcome

Trust fabric for interconnectivity and information exchange that is cost effective for all entities and protects all stakeholders by:

- Focusing on a risk management-based security approach
- Leveraging existing security frameworks and regulations to the maximum extent possible
- Creating a comprehensive, flexible, scalable security strategy for health care interconnectivity that:
  - Matches levels of security requirements, controls and compliance with the health care business and data interconnectivity work
  - Offers more than one approach to meet the security concerns of participating stakeholders
  - Requires definition of certain minimum threshold goals, such as ensuring information protection
  - Outlines a governance structure to support the overarching goals