Health IT Briefing to the Information Security and Privacy Advisory Board

Security Assurance Compliance between Federal and Non-federal Health Information Exchanges (HIE)

December 2, 2009

Federal Panelists

- **Ms. Jodi Daniel (Lead)**
  - ***Office of the National Coordinator (ONC)****; Director, Office of Policy & Planning*
- **Ms. Ashley Corbin**
  - ***Centers for Medicare & Medicaid Services (CMS)****; Director, Division of Requirements and Validation*
  - ***FHA Federal Security Strategy (FSS) Working Group****; Co-Chair*
- **Ms. Gail Belles**
  - ***Veterans Health Administration (VHA),*** *Director, Health Care Security Requirements*
- **Ms. Kitt Winter**
  - ***Social Security Administration (SSA)****; Director, HIT Strategic Resources, Office of the Commissioner*

Jodi Daniel

Director, Office of Policy & Planning,

Office of the National Coordinator (ONC)

Objectives

- Provide a context for the national health information technology (HIT) strategy
- Identify security framework implications to nationwide exchange of health information among Federal and non-Federal entities
- Share experiences from Federal entities
- Identify areas for guidance to simplify, promote uniformity and address possible barriers to nationwide health information exchange

American Recovery and Reinvestment Act of 2009 (ARRA)

- Congressional mandate that provides more than $20 billion to aid in the development of a robust IT infrastructure for healthcare and to assist providers and other entities in adopting and using health IT
  - $2 billion for the Office of the National Coordinator (ONC)
  - $18 billion in incentives through the Medicare and Medicaid reimbursement systems to assist providers in adopting EHRs
  - $85 million for health IT, including telehealth services, within the Indian Health Service
  - $500 million for the Social Security Administration
  - $50 million for information technology within the Veterans Benefits Administration

Health Information Exchange (HIE) Goals

- Foster the development of a “nationwide health information technology infrastructure that allows for the electronic use and exchange of information.”
- Enable secure information exchange between Federal and non-Federal entities to:
  - Improve health outcomes
  - Advance patient-centered health care
  - Reduce errors and health disparities
- Eliminate commercial, economic and technical barriers to the exchange of health information across jurisdictions.

Nationwide Health Information Exchange Model

- A nationwide model must accommodate and foster information exchange among diverse health care entities and organizations, including Federal and non-Federal entities

- Need platform for trust, security and privacy that will support and scale on a nationwide basis

Security Considerations for Nationwide Health Information Exchange

- Based upon applicable law and existing frameworks
  - For Federal entities – FISMA
  - For non-Federal entities that are Covered Entities and Business Associates – HIPAA
  - Other laws or frameworks – Privacy Act, ISO, etc.,
- Parties to the exchange may also establish additional expectations for trust, for example the DURSA
- Uniformity and compatibility will be essential for nationwide exchange of health information

Nationwide Health Information Network (NHIN)

- Currently, the NHIN is a network that ties other health networks together, across the internet, in a common, interoperable infrastructure
  - Assurances addressed through additional trust mechanisms
  - Technical requirements, including controlled participation
  - Accountability measures and governance
  - Robust trust agreement
- Additional information exchange models under consideration by the Health Information Technology Policy Committee

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 expectations for appropriate security of interfaces could simplify, add flexibility and scale to enable health information exchange to achieve goals of HITECH
- Longer-term, there is a need for a consistent nationwide information security posture for electronic health information exchange between Federal and non-Federal entities

Federal Partner Panel Discussion

Perspectives of the Panelists in terms of Challenges and Current Approaches

- Ashley Corbin, CMS, Federal Security Strategy WG
- Gail Belles, VHA
- Kitt Winter, SSA

Ashley Corbin

Director, Division of Requirements and Validation, Centers for Medicare & Medicaid Services (CMS)

Co-Chair, FHA Federal Security Strategy (FSS) Working Group

Key Areas for Guidance

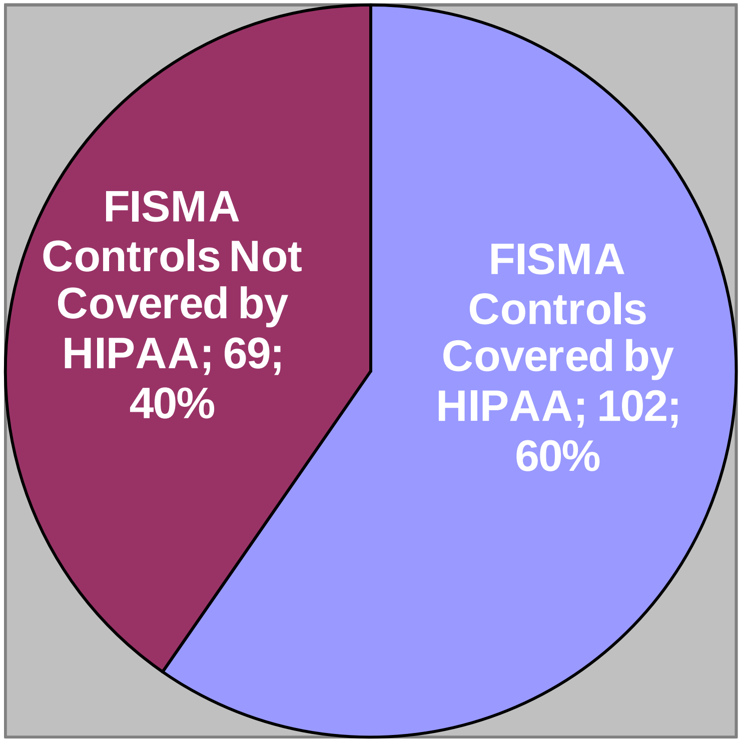
- Conceptual Variation between Security Frameworks; for example, Differences in the Treatment of System Interoperability
  - Benefit: Improved efficiency in security assurance evaluation, common understanding of comparative elements, approved security assurance level rating schema
- Policy Guidance which enables successful implementation to meet the President's health care agenda
  - Benefit: Industry-specific security and privacy expectations with limited variability will improve the number and quality of HIE implementations
- Recognition that Existing NHIN Tools Compliment the Federal Requirements
  - Benefit: Enable HIE growth through coordinated tool development that maps to policy & regulations and is strengthened by governance
- Harmonize Security Framework Models
  - Benefit: Short-term assistance aimed at augmenting accepted risk management techniques with clarity around variations in security controls and safeguards

FISMA and HIPAA Overlap

- FISMA and HIPAA are based on the same underlying principles of information system security, however:
  - Some Federal security controls were not addressed in HIPAA Regulations, such as Configuration Management
  - Some controls may not be applicable to the private sector, such as System Acquisition
  - Other differences are a matter of degree, such as Identification and Authentication
- NIST SP 800-66, Introductory Resource Guide for Implementing HIPAA Security Rule, Appendix D, provides a crosswalk between HIPAA Security Rule and NIST SP800-53
- How to do consistent comparative analysis of other security frameworks; ITIL, ISO, CoBIT, for ex.

Example of FISMA to HIPAA Comparative Analysis

NIST Analysis
FISMA Controls Covered by HIPAA



As defined by “FIPS PUB 199 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Standards for Security Categorization of Federal Information and Information Systems” used in context to describe potential impact … “The potential impact is MODERATE if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

Gail Belles

Veterans Health Administration (VHA), Director, Health Care Security Requirements

Veterans Administration

VA/KP NHIE Collaboration

- Overview
- Current Approach
- Challenges

AAMC-VA Research Data Exchange

- Overview
- Current Approach
- Challenges

Kitt Winter

Social Security Administration (SSA); Director, HIT Strategic Resources, Office of the Commissioner

Social Security Administration

- SSA completed the Security Risk Assessment process for its Health Information Technology Web Services Interface with the Nationwide Health Information Network CONNECT Gateway 1.0.

- The following slides detail steps taken to complete the risk assessment.

Social Security Administration

1) Reviewed and determined what data would be at risk.

2) Reviewed each NIST SP 800-53 (FISMA) control and highlighted those not covered by NIST SP 800-66 (HIPAA) and visa versa.

3) Assessed the possible impact to SSA of the potential lack of each of specific control, as well as, any compensating controls already in place.

4) Identified potential threat sources or vulnerabilities associated with the HITWSI 2.0 Release / NHIN CONNECT Gateway 1.0.

5) For each potential threats or vulnerabilities, assessed the possible risks and determined whether the compensating controls were in place commensurate with the level of risk.

6) Plan to reassess risk assessments as additional providers are added and systems updates are completed.

Desired Outcomes

- Federal agency participation in nationwide health information exchange is essential to achieving the goals of the HITECH Act and to improving care
- Guidance that promotes consistency and clarity should simplify the process, provide the necessary assurances and still enable secure, nationwide health information exchange with non-Federal entities
- Harmonizing the various security controls for HIE exchanges
- Allowing sufficient flexibility for individual Agency implementations
- Reducing the resource requirements for Federal efforts to identify and control security risks for HIEs
- Providing a mutual framework for Federal agencies to trust the security capabilities of private sector HIE participants