The Case for an Information Security Road Map for HIE and EHR

Ashley Corbin, PhD
Director, Division of Requirements and Validation, CMS Co-chair
Federal Security Strategy Work Group, ONC/FHA

Northern Virginia Technology Council (NVTC)

June 16, 2009
Agenda

- Health Information Exchange (HIE) and National Health Information Network (NHIN) Introduction
- What is unique about HIE and NHIN Security and Privacy?
- Federal NHIN Security and Privacy Initiatives
President Obama’s Commitment to Electronic Health Systems

The goal is not to move from “paper silos” to “electronic silos”

The goal is an electronic health system that **sustains and requires the movement of interoperable health information** supporting:

- Quality of Care
- Continuity of Care
- Population Needs (pandemics and other disasters)
- Bench to Bedside Research
- Disability Determination

*In a January 9, 2009 speech at George Mason University*

"To improve the quality of our healthcare while lowering its cost, we will make the immediate investments necessary to ensure that, within five years, all of America’s medical records are computerized.”
Vision - The Movement of Interoperable Health Information to Improve Health Outcomes and Cost
What is Unique about NHIN Security & Privacy?

- How can Federal agencies have security assurance when exchanging health information with non-federal entities?

- When information travels between Federal, and Non-Federal entities:
  - Who has stewardship and ownership responsibility for the data?
  - What security regulations apply?
  - What are the requirements and responsibilities for HIE and EHR security capabilities?
Why this Matters

Differences in information security laws, requirements, and policies in the federal and non-federal sectors impacts the expansion of electronic exchange of health information.

FSS Work Group was chartered to analyze and develop practical guidance, recommendations and a strategic roadmap to address the situation.
## Whose Data is It?

<table>
<thead>
<tr>
<th>Healthcare Facility</th>
<th>Data</th>
<th>Ownership</th>
<th>Applicable Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Treat Patient</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Submit Medicare Claim</td>
<td></td>
<td>Clinical Data (Chart, Notes, Labs, etc)</td>
<td>Healthcare Facility</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Billing Data</td>
<td></td>
</tr>
<tr>
<td>Submit Information to HIE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process Medicare Claim</td>
<td></td>
<td>Medicare Claim</td>
<td>CMS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HIPAA rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FISMA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CMS</th>
<th>Data</th>
<th>Ownership</th>
<th>Applicable Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Health Information Exchange</th>
<th>Data</th>
<th>Ownership</th>
<th>Applicable Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add Medicare information to patient medical record</td>
<td></td>
<td>Medicare data appended to clinical record</td>
<td>????????????????</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clinician</th>
<th>Data</th>
<th>Ownership</th>
<th>Applicable Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Patient EHR Record</td>
<td></td>
<td>Clinical Record</td>
<td>Provider?</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HIPAA Rules</td>
</tr>
</tbody>
</table>
What Security Regulations Apply?

- Federal agencies and its contractors must follow FISMA
- Private sector follows HIPAA Privacy and Security rules

• FISMA
  - NIST SP 800-53 (Security Controls for Federal Information Systems and Organizations)
  - The Joint Commission
    - EC 2.10.7 Implements Incident Procedures
    - IM 2.20 Maintains Security/Integrity
    - IM 2.30 Provides For Continuity of Information
  - HIPAA
    - 164.308 (a)(6) Security Incident Procedures (R)
    - 164.308 (a)(7)(ii)(D) Contingency Testing/Revision Procedures
    - NIST SP 800-66 Security Rule
  - SOX
    - Manage Problems & Incidents; A Process Exists to Support
      - Timely Response & Investigation of Unauthorized Activities

• COBIT
  - DS5.6 Security Incident Definition
  - DS10.1 ID & Classification of Problems
  - DS10.3 Problem Closure
  - ISO17799
    - 8.2.3 Disciplinary Process
    - 13.1.1 Reporting InfoSec Events
    - 13.1.2 Reporting Security Weaknesses
    - 13.2.1 Responsibilities & Procedures
    - 13.2.2 Learning From InfoSec Incidents
    - 13.2.3 Collection of Evidence
  - ISO/IEC 27000:2005
    - ISO 17799:2005
    - PCI
      - 11.1 (a-c) Regular Testing of Systems & Processes (wireless)
      - 12.5.3 Maintaining InfoSec Policy (Response & Escalation Procedures)
      - 12.9.1-6 Incident Response Plans; Annual Testing, Training,
        - Personnel, Evolution via Lessons Learned
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
Does FISMA Apply to the Private Sector when Exchanging Health Information with Federal Agencies?

The purpose of FISMA:

- **A comprehensive framework** for ensuring the effectiveness of information security controls over information resources that support Federal operations.

- **Recognize the highly networked nature of the current Federal computing environment** and provide effective government wide management and oversight.

§3544 Federal agency responsibilities

- **Agencies must provide information security for the information and information systems that support the operations and assets under their control.**

- **Agencies must provide information security protections commensurate with the risk for**:
  - Information collected or maintained **by or on behalf of** the agency; and
  - Information systems **used or operated by** an agency
  - Information systems **used on behalf of** an agency (e.g., by a contractor)

A New Paradigm

- **Traditional View of Data Ownership**
  - The possession of information.
  - Implies control and responsibility for the integrity and security of information.
  - NHIN/HIE challenges this traditional mindset.

- **Towards Information Stewardship**
  - Information owner may not be the most appropriate concept since citizens ultimately own the information.
  - Responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that originated.
  - Provide access to federal information for customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.

Source: NIST SP 800-37, Rev 1
To establish a trust fabric for the NHIN/HIE 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
What are the requirements and responsibilities for HIE security capabilities?

**Integrity**
Prevention of unauthorized modification of data.
- Identification
- Non Repudiation
- Accountability

**Confidentiality**
Prevention of unauthorized disclosure of data.
- Encryption
- Audit Logs
- Time Recording
- Authentication
- Authorization / role-based access

**Availability**
Prevention of loss of access to resources and data.
- Service Level Agreement
- Continuity of Operations (COOP/DR)
- Recovery Time Objective
- Recovery Point Objective

- What expectations do participants have for HIEs/NHIN related to these capabilities?
- What do HIEs/NHIN expect from participants related to these security capabilities?
- Who should detect non-conformance with security requirements? How to enforce adherence to requirements?
Trust and assurance are the primary focus

- Security controls
- Monitoring compliance of organizations and individuals nationwide
- Data ownership

A service model approach

- Security standards – NIST, OMB, HITSP
- Certification of products – CCHIT, HITRUST
- Data use agreements – NHIN DURSA, agency specific DUAs
- Site Monitoring for compliance (e.g., HI-TRUST, lottery)
- Governance
Information Security Service Model
Approach

- Use standards-based certified products
- Establish public and private collaborative to ensure compliance is achieved and maintained for the varying implementations of the certified products
- Leverage each organization’s capabilities for contributions in an overall governance framework
- Each participant is assessed their fair share of cost
- Periodicity of evaluation, certification, and compliance based on a minimum set of criteria, but adaptable to the changing circumstances (e.g., the local HIEs)
- Coordinate overall critical success factors and a process for continuous improvement
The FSS Work Group has drafted interim guidance for the federal partners that focuses on risk management-based adequate security assurances under FISMA.
Action Directives – Roadmap

- Builds on the Security and Privacy Framework for Electronic Exchange of Individually Identifiable Health Information released December 15, 2008 by HHS and identifies actions that HIE participants can take to manage security risk

- Provide recommendations for building a secure HIE infrastructure and building and managing trust

- Identify and recommend standards, policies, guidance and associated artifacts to support the end-to-end security posture for all users