WEDi
Workgroup for Electronic Data Interchange

NIST / URAC / WEDi Health Care Security Workgroup

Presented by:
Andrew Melczer, Ph.D.
Illinois State Medical Society

Background

- NIST/URAC/WEDi Health Care Security Workgroup established late 2002
- Response to HIPAA final Security Rule
- Formed to:
  - Facilitate identification and implementation of best practices in health care for information security requirements
  - Identify similarities between those practices and HIPAA standards

Workgroup Mission

- To facilitate communication and consensus on best practices for information security in health care
- To promote implementation of uniform approach to security practices and assessments

Workgroup Goals

- Identify security standards for future use in health care industry
- Review and discuss security standards currently being used in health care industry to drive consensus on best practice

Founding Organizations

- Three founding organizations
  - NIST
  - URAC
  - WEDi

Workgroup for Electronic Data Interchange

NIST

- National Institute of Standards and Technology
- Founded in 1901
- Non-regulatory federal agency
- Within U.S. Commerce Department's Technology Administration

Workgroup for Electronic Data Interchange

NIST

- Mission: To develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life
- Responsibilities include development of technical, physical, administrative, and management standards and guidelines for cost-effective security and privacy

Workgroup for Electronic Data Interchange

URAC

- Independent, nonprofit organization
- Leader in promoting health care quality through accreditation and certification
- Offers wide range of quality benchmarking programs and services
- Provides symbol of excellence for organizations to validate commitment to quality and accountability
- Ensures all stakeholders represented in establishing quality measures

WEDi

- Workgroup for Electronic Data Interchange
- Vision: Improve health care through electronic commerce
- Mission: Foster widespread support for the adoption of electronic commerce within health care

WEDi

- Provides forum for definition of standards, resolution of implementation issues, development and delivery of education and development of strategies and tactics for continued expansion of electronic commerce in health care
- Named in HIPAA as one of entities HHS directed to consult

HC WG Founding Organization Contacts

- Lisa Gallagher, URAC
  (lgallagher@urac.org)
- Arnold Johnson, NIST
  (arnold.johson@nist.gov)
- Mark McLaughlin, WEDi
  (mark.mclaughlin@mckesson.com)

Work to Date

- Workgroup holds meetings nearly every month
- Covered great deal of information
- Information on all past and future Workgroup meetings at:

  www.urac.org/committees_sworkgroup.asp

Work to Date

- HIPAA Security Rule
- Meeting Safeguard Requirements in Privacy Rule (Section 164.530(c))
- NIST SP 800-30: *Risk Management Guide for Information Technology Systems*
  - Describes how to perform a risk analysis
  - 4 NIST documents cited in final Security Rule

Work to Date

- NIST SP 800-37: *Guide for the Security Certification and Accreditation of Federal Information Systems*
  - Being developed in response to Federal Information Security Management Act of 2002
- NIST SP 800-53: 1st draft: *Recommended Security Controls for Federal Information Systems*
  - Recommended set of controls for low and moderate impact systems

Work to Date

- Security Self-Assessment Guide for IT Systems and the Automated Security Self-Evaluation Tool (ASSET)
  - Purpose to automate completion of questionnaire in NIST SP 800-26
  - Users able to assess IT security posture for systems and assess status of organization's security program plan

Work to Date

- FIPS (Federal Information Processing Standards) Publication 199: *Standards for Security Categorization of Federal Information and Information Systems*
  - FIPS Publications meant to apply to federal government agencies
  - Defines baseline for security categorization standards and potential levels of risk relevant to securing federal information and information systems

Work to Date

- ISO 17799 Security Standards: *Information Technology – Code of Practice for Information Security Management*
  - Detailed security standard organized into ten major sections, each covering a different topic or area
  - ISO = International Organization for Standardization sells ISO 17799

Work to Date

- CMS Contractor Assessment Security Tool (CAST)
  - Provides Medicare Carriers and Intermediaries with standard method of documenting compliance with CMS Core Security Requirements
- CMS Internet Security Requirements
  - Establishes fundamental rules and system security requirements for use of Internet

Workgroup for Electronic Data Interchange

Work to Date

- SEI OCTAVE Model for Risk Analysis
  - Risk-based strategic assessment and planning technique for security
- HIPAA-CMM proposed by Corbett Technologies
  - Standard methodology for assessing health care organization's compliance with HIPAA security standards
- And more ….

Disclaimer

- Workgroup does not endorse and is not suggesting that entities use any specific products described above, including those for sale only
- Rather, Workgroup reviewing range of products in order to develop guidance for industry in implementing HIPAA Security Rule

Work Plan

- Crosswalk Task Force established
- Provide crosswalk of HIPAA Security Rule requirements to existing security standards used in health care
- Provide industry with crosswalk matrix to assist with effective implementation of HIPAA by comparing various security standards, which may already be implemented, with HIPAA

Workgroup for Electronic Data Interchange

Crosswalk

- Focus of remainder of afternoon
- Standards being considered for review:
  - NIST Special Publication 800 Series
  - ISO 17799
  - CMS Core Security Requirements
  - CMS Internet Security Requirements
  - Federal Information System Control Manual (FISCAM)
  - DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

Resources

- URAC for Workgroup information, minutes, and presentations

  www.urac.org/committees_sworkgroup.asp
- NIST for SP 800 Series

  csrc.nist.gov/publications/nistpubs/index.html
- WEDi for Security White Papers, including summary of NIST SP 800 documents

  www.wedi.org/snip/public/articles/index%7E10.htm

Andrew H. Melczer, Ph.D.
Vice President, Health Policy Research
Illinois State Medical Society
melczer@isms.org