



Workgroup for
Electronic Data Interchange

Security Requirements Crosswalk

NIST/URAC/WEDI Healthcare Security Workgroup

Presented by Mike Bell,

Bruce Gnatowski, Carla Dancy Smith,

Adam Stone, and Ken Yale



Workgroup for
Electronic Data Interchange

Table of Contents

- ▶ Crosswalk Defined (What we are doing?)
- ▶ Process (How are we approaching?)
- ▶ Participants (Who are the Volunteers?)
- ▶ Timelines (When will industry review take place?)
- ▶ Next Steps



Workgroup for
Electronic Data Interchange

Crosswalk

- ▶ “Crosswalk” defined: Analysis of various requirements – aka “security traceability matrix”
- ▶ Crosswalk analysis purpose:
 - Identify and leverage other, similar security requirements, and
 - Identify HIPAA Security measures that may already be satisfied by current practices
- ▶ Final crosswalk template, with analysis, can be used as a tool to assist an organization in supporting ROI of previous security initiatives and how they interface with HIPAA compliance



Workgroup for
Electronic Data Interchange

Crosswalk Process

- ▶ HIPAA Security Rule as Driver
- ▶ Goal: To capture the correlation of the HIPAA security rule to the referenced standard
- ▶ Disclaimers and assumptions will be stated
 - Crosswalk analysis theoretical and high-level
 - HIPAA compliance will not substitute or negate the compliance with other regulations
 - An organization is responsible for using the crosswalk as a tool in developing their compliance plan and not as a compliance mechanism
 - The crosswalks are draft discussion documents, not to be taken as legal advice or viewed as approved industry standards



Workgroup for
Electronic Data Interchange

Crosswalk Leadership

▶ **Leadership**

- Lisa Gallagher, URAC
- Dr. Ron Ross, NIST
- Mark McLaughlin, WEDI

▶ **Co-Chairpersons**

- Carla Smith, Booz, Allen, Hamilton
- Denise Turner, NYS OMRDD HVDDSO
- Dr. Ken Yale DDS, JD EduNeering
- Bob Perlitz, Healthcare IS Consultants



Workgroup for
Electronic Data Interchange

Crosswalks Sub Group Assignments

NAME	STANDARD
Carla Smith, Booz Allen Hamilton	NIST 800 - Series
Mike Fisher, Daou, Inc.	ISO - 17799
Adam Stone, Fortis	ISO - 17799
George Goble, Trinity Health	ISO - 17799
Bruce Gnatowski, AMS	CMS - CSR
Mike Cummings, TecSec	CMS - CSR
Dennis Seymour, VHA	FISMA
Jon Bogen, HealthCIO	CMS Internet Security
Dennis Seymour, VHA	JCAHO
Cass Solomon, Kinder HealthCare	Octave



Workgroup for
Electronic Data Interchange

Timelines and Next Steps

- ▶ Crosswalk template and standards developed
- ▶ Review for internal consistency and completeness
- ▶ Draft available for review in April
- ▶ Comment period commences – Spring 2004
- ▶ Peer review process begun – Summer 2004
- ▶ Final industry consensus document – Fall 2004



Workgroup for
Electronic Data Interchange

Example



Workgroup for
Electronic Data Interchange

Example of Training Standard



Workgroup for
Electronic Data Interchange

HIPAA Section 164.308(a)(5)(i)

- ▶ Addressable: Implement a security awareness and training program for all members of the workforce (including management).
- ▶ Implementation Specifications:
 - ▶ Security reminders - Periodic security updates
 - ▶ Protection from malicious software - Procedures for guarding against, detecting, and reporting malicious software
 - ▶ Log-in monitoring - Procedures for monitoring log-in attempts and reporting discrepancies.
 - ▶ Password management - Procedures for creating, changing, and safeguarding passwords.



Workgroup for
Electronic Data Interchange

ISO 17799 Standard 6.2.1

- ▶ Information security training and education: Ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work
- ▶ Note: “Code of practice” gives high-level, general descriptions of policies and general good practices
- ▶ “Does not currently cover all areas of importance” but is being revised – NIST, November 2002



Workgroup for
Electronic Data Interchange

CMS Core Security Requirements

1.1.1

- ▶ Management and Staff shall receive security training, security awareness, and have security expertise
 - ▶ Awareness training
 - ▶ Periodic security reminders
 - ▶ User education concerning malicious software
 - ▶ User Education in importance of monitoring log-in success/failure and how to report discrepancies
 - ▶ User education on password management

CMS Core Security Requirements Other

- ▶ Security awareness training customized, based on job responsibilities
- ▶ Employees acknowledge having received training
- ▶ Record of the security awareness training
- ▶ Training in emergency procedures
- ▶ Training to ensure copyright information is protected
- ▶ Trained to challenge people not recognized
- ▶ Information on restrictions against unauthorized activities and accesses
- ▶ Employees shall understand their security duties and responsibilities



Workgroup for
Electronic Data Interchange

NIST Special Publication 800-16

- ▶ Guidelines for Federal computer security training
- ▶ Computer Security Basics
- ▶ Security Planning and Management
- ▶ Computer Security Policies and Procedures
- ▶ Contingency Planning
- ▶ Systems Life Cycle Management
- ▶ Target Audiences:
 - ▶ Executives
 - ▶ Program/Functional Managers
 - ▶ IRM Security and Audit
 - ▶ ADP Management and Operations
 - ▶ End Users



Workgroup for
Electronic Data Interchange

Contact Information

- ▶ Contact a Co-Chair for more information:
 - Ken Yale, EduNeering, Inc. 609-947-3820
 - Carla Smith, Booz Allen Hamilton, 703-289-5936
 - Denise Turner, New York State Government, 845-947-6064
 - Bob Perlitz, healthcare IS Consultants, 917-664-4707
- ▶ Questions and Answers??