The CPRI Toolkit: Managing Information Security in Health Care
And other HIPAA Tools

Jeff Collmann, PhD
Associate Professor
Department of Radiology
Georgetown University

Ted Cooper, MD
National Director
Confidentiality & Security
Kaiser Permanente
HIPAA Security & Privacy Standards Requirements

• We must
  – Perform and thoroughly document formal risk assessment and management efforts to determine the policies, procedures and technology to deploy to address the standards.
  – We must assess the types and amounts of risk that we have, which we will mitigate with policy, procedure and/or technology, and understand what risks remain and that we are willing to accept (i.e. those that will not be addressed completely)
  – Assign responsibility for meeting the standards to specific individuals.
HIPAA Standards for Security & Privacy

While these are called the HIPAA Security and Privacy Standards, the “standard” simply means that we must address their requirements. For the most part both standards are not explicit on the extent to which a particular entity should implement specific policies, procedures or technology. Instead, they require each affected entity to assess its own security and privacy needs and risks and then devise, implement and maintain appropriate measures as business decisions.
HIPAA Standards for Security & Privacy

• Was not issued in August
• When will they be issued?
  – Rumors
  – Guesses
• When do the final rules become effective?
Tools

- CPRIToolkit: Managing Information Security in Health Care
- NCHICA’s HIPAA EarlyView™
- SEI’s Self Risk Assessment Tool
- WEDI’s HIPAA Security Summit Implementation Guidelines
The CPRI Toolkit: Managing Information Security in Health Care

• How to use it to address HIPAA confidentiality and security
CPRI Toolkit
Original Task Force 1998

• Ted Cooper, MD - task force chair
• Jeff Collmann, PhD - editor
• Barbara Demster, MS, RRA
• Keith MacDonald
• Susan K. Odneal, CISSP
• Jeanne Reiners
CPRI Toolkit

Content Committee 2000

- Ted Cooper, M.D., Chair
- Jeff Collmann, Ph. D., Editor
- Barbara Demster, MS, RRA - Healtheon/WebMD
- John Fanning - DHHS
- Jack Hueter - CHE
- Shannah Koss - IBM
- Elmars “Marty” Laksbergs, CISSP - Netigy
- John Parmigiani - HCFA
- Harry Rhodes - AHIMA
- Paul Schyve, MD - JCAHO
CPRI Toolkit

- Third Version of Toolkit - May 2000

- http://www.cpri-host.org
Goal

Build security capable organizations!
Incorporate sound security practices in the everyday work of all members of the organization, including the patient. NOT JUST Implementing security measures!
Security Program Functions

• Monitor changing laws, rules and regulations
• Update data security policies, procedures and practices
• Chose and deploy technology
• Enhance patient understanding and acceptance
How does the *Toolkit* help?

- Regulatory requirements
- CPRI booklets
  - How to go about it
  - What to consider
- Case studies & examples of colleagues’ work
Table of Contents

CPRI Toolkit: Managing Information Security in Health Care, Version 2

HTML Table of Contents

1.0 Executive Summary
2.0 Introduction
   2.1 How to Use This Toolkit
3.0 Monitoring Laws, Regulations, and Standards
   3.1 Introduction
   3.2 Summary of Proposed DHHS Rules
      3.2.2 Common Elements
      3.2.3 Proposed Data Security and Electronic Signature Standards
      3.2.4 Electronic Transactions/Code Sets
      3.2.5 Health Care Provider Identifier
Download Center

CPRI Toolkit: Managing Information Security in Health Care, Version 2

PDF Table of Contents
The Document Download Center has been provided for your printing convenience. In order to download the PDF files you will need to download the Adobe Acrobat Reader. A link to the Acrobat Reader has been provided below.

CPRI Toolkit by sections

1.0 Executive Summary
2.0 Introduction
  2.1 How to Use This Toolkit
3.0 Monitoring Laws, Regulations, and Standards
  3.1 Introduction
  3.2 Summary of Proposed DHHS Rules
    3.2.2 Common Elements
    3.2.3 Proposed Data Security and Electronic Signature Standards
    3.2.4 Electronic Transactions/Code Sets
    3.2.5 Health Care Provider Identifier
    3.2.6 Employer Identifier
    3.2.7 Health Plan Identifier
    3.2.8 Unique Health Identifier - Individuals

 Entire CPRI Toolkit (1.8MB, Apx. 505pp)
Toolkit - Sections 1 & 2
3.0 Monitoring Laws, Regulations, and Standards
   3.1 Introduction
   3.2 Summary of Proposed DHHS Rules
      3.2.2 Common Elements
      3.2.3 Proposed Data Security and Electronic Signature Standards
      3.2.4 Electronic Transactions/Code Sets
      3.2.5 Health Care Provider Identifier
      3.2.6 Employer Identifier
      3.2.7 Health Plan Identifier
      3.2.8 Unique Health Identifier - Individuals
   3.3 Final Federal HIPAA Security & Electronic Signature Standard
   3.4 Federal Medical Privacy Legislation
      3.4.1 Summary of DHHS Confidentiality Recommendations
      3.4.2 Privacy Notice of Proposed Rule Making
   3.5 State Medical Privacy Legislation
   3.6 Setting Standards in Health Care Information (12/15/1999)
   3.7 JCAHO/NCQA Recommendations for Protecting Personal Health Information

October 2000 17
Toolkit - Section 4.0 - 4.5.2

4.0 Developing Policies, Procedures, and Practices

4.1 Introduction

4.2 CPRI Guidelines - Information Security Policies

4.3 Sample Security Policies

4.3.1 Harvard Vanguard Medical Associates

4.3.2 Kaiser Permanente Northern California

4.3.3 Mayo Clinic

4.3.4 Partners Healthcare System

4.3.5 PCASSO Security Policy Model

4.3.6 Project Phoenix, Georgetown University

4.4 Assigning Roles and Responsibilities

4.4.1 Introduction

4.4.2 CPRI Guidelines for Managing Information Security Programs

4.4.3 Case Study: Immunization Information Systems at University of Pennsylvania

4.5 Conducting Data Security Risk Analyses

4.5.1 Case Study: Project Phoenix - Risk Analysis of a Telemedicine System

4.5.2 Case Study: Project Phoenix - Risk Management Plan
**Toolkit - Section 4.6 - 4.9.3**

<table>
<thead>
<tr>
<th>4.6 Organizing Security Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6.1 CPRI Guide - Information Security Education</td>
</tr>
<tr>
<td>4.6.2 Sample Training Materials</td>
</tr>
<tr>
<td>4.6.2.1 Instructor Guide</td>
</tr>
<tr>
<td>4.6.2.2 Slides for Training Program (Online View)</td>
</tr>
<tr>
<td>4.6.2.2 Slides for Training Program (Download Powerpoint)</td>
</tr>
<tr>
<td>4.6.3 Conferences on Information Security Training</td>
</tr>
</tbody>
</table>

| 4.7 Additional Resources |

<table>
<thead>
<tr>
<th>4.8 Enforcing Security Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.8.1 CPRI Sample Confidentiality Statements &amp; Agreement</td>
</tr>
<tr>
<td>4.8.2 Case Study: Securing User Agreement at Kaiser Permanente Northern California</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4.9 Implementing Information Security Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.9.1 CPRI Guide — Security Features</td>
</tr>
<tr>
<td>4.9.2 Special Issues in Electronic Transmission of Confidential Data</td>
</tr>
<tr>
<td>4.9.2.1 Fax — Special Issues in Electronic Transmission</td>
</tr>
<tr>
<td>4.9.2.2 Email</td>
</tr>
<tr>
<td>4.9.2.3 HCFA and the Internet</td>
</tr>
<tr>
<td>4.9.3 Case Study: Patient Centered Access To Secure Systems Online (PCASSO)</td>
</tr>
</tbody>
</table>

October 2000
5.0 Enhancing Patient Understanding
   5.1 Introduction
   5.2 Complying with Consent, Inspection, and Disclosure Requirements
   5.3 HelpBot: Complying with Patient Education Requirements

6.0 Institutionalizing Responsibility
   6.1 Introduction
   6.2 Case Study: Trustee/Custodian Agreements at Kaiser Permanente

7.0 Web Sites
8.0 Glossary
9.0 Bibliography
Managing Information Security in Health Care

- Policy = what you want done
- Procedure = how is it should be done
- Technology used to enforce policies & procedures through automation
- Practice = what is done - audit

Requires a Plan

- The plan should address all four
Critical Steps in Process

1. Decide what to do
2. Assign security responsibilities
3. Build risk management capability
4. Drive enterprise-wide awareness
5. Enforce policies & procedures
6. Design, revise & validate infrastructure
7. Institutionalize responsibility & support
8. Enhancing patient understanding

HIPAA Deadline: 2002-2003
1. Deciding what to do

- *Understand the Regulations* - 3
- *Information Security Policies* - 4.2
  - Describes how to develop policies
  - Identifies areas policies should address
  - Security policy examples - 4.3.1 to 4.3.6
Know the Laws, Rules & Regulations

• HIPAA
  – Data Security Rules - 3.1
  – Federal Medical Privacy - 3.2

• State Medical Privacy Laws - 3.3

• Setting Standards - 3.4

• JCAHO/NCQA Recommendations - 3.5

• New: EU Privacy Directive - “Safeharbor”
Information Security Policies

- HCFA
  - Barbara Clark
    - Senior Systems Analyst
  - 4.2 CPRI Guidelines - Information Security Policies
  - 4.3 Sample Security Policies
    - 4.3.1 Harvard Vanguard Medical Associates
    - 4.3.2 Kaiser Permanente Northern California
    - 4.3.3 Mayo Clinic
    - 4.3.4 Partners Healthcare System
    - 4.3.5 PCASSO Security Policy Model
    - 4.3.6 Project Phoenix, Georgetown University

- JCAHO
  - Paul Schyve, MD
    - 4.3.3 Mayo Clinic

- 3Com Corporation
  - Bill Sherman
    - Content Manager,
    - 4.3.6 Project Phoenix, Georgetown University
Toolkit & Critical Steps

2. Assigning Roles and Responsibilities

- Managing Information Security Programs
  - CPRI Guide on management processes - 4.4.2
  - Case Study of UPenn electronic registry - 4.4.3
Managing Information Security Programs

4.4.2 CPRI Guidelines for Managing Information Security Programs

4.4.3 Case Study: Immunization Information Systems at University of Pennsylvania
Toolkit & Critical Steps

3. Building Risk Management Capability

• CPRI Toolkit - 4.5
  – New Health Information Risk Assessment and Management
    • Software Engineering Institute
  – Risk assessment - 4.5.1
  – Risk management plan - 4.5.2
Building Risk Management Capability

4.5 Conducting Data Security Risk Analyses

4.5.1 Case Study: Project Phoenix - Risk Analysis of a Telemedicine System

4.5.2 Case Study: Project Phoenix - Risk Management Plan
4. Driving enterprise-wide awareness

- *Information Security Education* - 4.6.1
  - CPRI Guide on security training
  - Sample Instructor’s guide and slides - 4.6.2
Information Security Education

4.6 Organizing Security Training
   4.6.1 CPRI Guide - Information Security Education
   4.6.2 Sample Training Materials
      4.6.2.1 Instructor Guide
      4.6.2.2 Slides for Training Program (Online View)
      4.6.2.2 Slides for Training Program (Download Powerpoint)
   4.6.3 Conferences on Information Security Training
   4.7 Additional Resources
Toolkit & Critical Steps

5. Enforcing Security Policies

- Confidentiality Statements - 4.8
  - Harvard Vanguard Policies - 4.3.1
  - Mayo Clinic Policies - 4.3.3
  - Kaiser Reaccreditation Process - 4.8.2
Enforcing Security Policies

4.8 Enforcing Security Policies

4.8.1 CPRI Sample Confidentiality Statements & Agreement

4.8.2 Case Study: Securing User Agreement at Kaiser

Permanente Northern California
**Toolkit & Critical Steps**

6. Implementing Security Infrastructure

- *CPR Guide on Security Features* - 4.9.1
- Special Issues in electronic media - 4.9.2
  - Fax, email
  - HCFA Internet Policy
  - Technology for securing the Internet
  - **New**: Connecticut Hospital Association PKI
  - **New**: Business Continuity Planning & Disaster Recovery Planning - 4.10
Implementing Security Infrastructure

- 4.9.1 CPRI Guide — Security Features
- 4.9.2 Special Issues in Electronic Transmission of Confidential Data
  - 4.9.2.1 Fax Special Issues in Electronic Transmission
  - 4.9.2.2 Email
  - 4.9.2.3 HCFA and the Internet
- 4.9.3 Case Study: Patient Centered Access To Secure Systems Online (PCASSO)
Toolkit & Critical Steps

7. Institutionalizing Responsibility

• Kaiser’s Trustee-Custodian Agreement
Institutionalizing Responsibility

6.0 Institutionalizing Responsibility

6.1 Introduction

6.2 Case Study: Trustee/Custodian Agreements at Kaiser Permanente
8. Enhancing Patient Understanding

• Toolkit - Section 4.3.4
  – Partners Healthcare System, Inc.

• Toolkit - Chapter 5.0
  – AHIMA Forms
  – HelpBot - Georgetown University
Enhancing Patient Understanding

5.0 Enhancing Patient Understanding

5.1 Introduction

5.2 Complying with Consent, Inspection, and Disclosure Requirements

5.3 HelpBot: Complying with Patient Education Requirements
Results

Enhanced judgement in managing health information

Improved health care information security
HIPAA Security Assistant

- Microsoft Access Database Application
- Displays each HIPAA Security
  - Requirement & Implementation Feature
  - One at a time
- Provides for your entry of
  - Items needed to be done to address each
  - A description of each item
HIPAA Security Assistant

• Future CPRI-HOST Product
• Focus Groups are being conducted
  – Contribute Content
• Analysis will be done to determine which items are common
• Can provide output in
  – MS Access Reports
  – MS Word file
  – MS Excel file
Disclaimer

The HIPAA Security Assistant should only be used as an aid to identify and define what needs to be done by your organization to become HIPAA compliant.

The example statements provided in the sample database should not be adopted by any organization without review by the individual responsible for confidentiality and security, the organization’s legal council and those with authority to set policy.

CPRI-HOST accept no responsibility for losses incurred through the use of the HIPAA Security Standard Assistant.
(1) The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.

<table>
<thead>
<tr>
<th>Concept</th>
<th>Description of What Needs to Be Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certification method</td>
<td>To perform the certification method to evaluate software, databases and networks is needed.</td>
</tr>
<tr>
<td>Authority for performing the technical assessment</td>
<td>The individual who is responsible for performing the technical assessment for certification must be explicitly stated.</td>
</tr>
<tr>
<td>Authority for accepting residual risk</td>
<td>The corporate officer responsible for accepting any residual risk for systems or networks which do not completely meet the set of certification requirements.</td>
</tr>
<tr>
<td>Level of software risk</td>
<td>Each software application and reporting database containing patient identifiable information will be classified for level of risk of unauthorized use or disclosure.</td>
</tr>
<tr>
<td>Level of network risk</td>
<td>Each computer network will be classified for level of risk of unauthorized disclosure.</td>
</tr>
<tr>
<td>Periodically</td>
<td>Each software application and network will be recertified no less than every 3 years.</td>
</tr>
<tr>
<td>Before implementing a system or connecting to a new network</td>
<td>A certification evaluation will be performed before connecting any software application or additional network to the Kaiser Permanente network.</td>
</tr>
<tr>
<td>When system is changed</td>
<td>A certification update will be performed with each release of an application.</td>
</tr>
<tr>
<td>Inventory of software and networks</td>
<td>An up to date inventory of all software applications, reporting databases and networks will be maintained.</td>
</tr>
</tbody>
</table>
HIPAA Proposed Security Regulation Self-evaluation Tool

www.nchica.org
Uses of *HIPAA EarlyView™*

- Staff education
- Gap analysis
  - Inadequate or missing policies
  - Previously unidentified vulnerabilities
- Due diligence documentation
- Budget planning
Greeting

NCHICA

HIPAA EarlyView™

Version 1.0

HIPAA Security Proposed Regulation Self-Evaluation Tool

http://www.nchica.org
919-558-9258

Copyright 2000 NCHICA All Rights Reserved
Main Menu

HIPAA EarlyView™

Start New Questionnaire
Update Existing Questionnaire
Run Reports
About HIPAA EarlyView(TM)
Exit

Copyright© 2000 NCHICA

All Rights Reserved
Enter Contact Data

HIPAA Security Questionnaire Contact Data

- Department Name: sample1
- Organization: Org
- Division: Div
- Cost Center: CC
- Project Lead: Proj Lead
- Title: Title
- Address1: Addr1
- Address2: Addr2
- City: City
- State: ST
- Phone: (999) 999-9999 Ext.
- E-Mail: email@sample.com
- Zip: 99999-9999
- Fax: (999) 999-9999
- Start Date: 1/1/00
- Due Date: 12/31/00
- Facilitator: Facilitator
- Title: Title
- F. Phone: (999) 999-9999 Ext.
- F. E-Mail: facilitator@sampel.com
- Serial #: 1234

Copyright © 2000 North Carolina Healthcare Information and Communications Alliance, Inc. All Rights Reserved
Update Questionnaire Menu
Security Questions

This form is used by a facilitator to conduct the HIPAA Security Questionnaire. It is designed to be used to capture all required information. Comments should be forwarded to DataSecurity@NCHICA.ORG. Thanks!

Question 1

Has an external entity or group performed a technical evaluation for BOTH your information systems AND network design for compliance with security standards?

Answer: [ ] Yes [ ] No [ ] N/A [ ] Unanswered

Due Diligence Demonstrated: [ ] Check if YES

Comments: evaluation done by test org - June 1999

Refer To:

Document Name: tech eval

Doc Type: Paper

Periodically Reviewed? [ ] No

Document Location:

Next Review Date (MM/DD/YYYY): 

Point of Contact: Mr. Contact

Contact Title: boss

Contact FAX: (999) 999-9999

Answer Date (M/D/Y): 6/9/00

Readress Requirement: [ ]
Report Menu

Run Reports for sample1

- Questions Unanswered
- Answers by HIPAA Table
- Master Question Listing by Implementation
- Master Questions and Answers
- Master Questions Referred To
- Questions Answered with "N/A"
- Questions Answered with "No"
- Questions Answered with "Yes"
- Questions to Readdress

NCHICA

Copyright © 2000 NCHICA All Rights Reserved
## Questions answered with "NO"

<table>
<thead>
<tr>
<th>HIPAA Table</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### HIPAA Implementation

<table>
<thead>
<tr>
<th>Question Number</th>
<th>Detailed Question</th>
<th>Refer To:</th>
<th>Contact</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Does your organization have an internal audit group that performs technical evaluations for BOTH information systems AND network design for compliance with security standards?</td>
<td>Susan Reference</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Available on the NCHICA Web site:
$150 license fee per site
($50 per site for NCHICA members)

www.nchica.org
Information Security Risk Assessments: A New Approach

- Christopher Alberts
- Team Leader
  - Security Risk Assessments

- Software Engineering Institute
- Carnegie Mellon University
- Pittsburgh, PA 15213

- Sponsored by the U.S. Department of Defense
Self-Directed IS Risk Assessments

• Goals:
  – To enable organizations to direct and manage risk assessments for themselves
  – To enable organizations to make the best decisions based on their unique risks
  – To focus organizations on protecting key information assets
Why a Self Directed Approach?

- SEI’s experience
  - Acting as external resource
    - Identify specific problems
    - Provide “laundry list” of items to be fixed
    - Fixes applied by organization
    - Next assessment similar issues identified
    - Root cause of issues remained
Why a Self Directed Approach?

• SEI’s experience
  – Sees need for organizations to internalize risk assessment
    • approach
    • education/knowledge
    • practices
    • instill a change in culture
Benefits

• Organizations will identify information security risks that could prevent them from achieving their missions.

• Organizations will learn to direct information security risk assessments for themselves.

• Organizations will identify approaches for managing their information security risks.

• Medical organizations will be better positioned to comply with HIPAA requirements.
SEI’s Self Risk Assessment

- Aimed at moderate to large sized organizations
- Methodology
- Team
- Workshops
  - Senior Management, Middle Management, Staff
  - Structured process
  - Catalogue of specific references
  - Outcome - choices support mission
IS Risk Assessment

Organizational View
- Assets
- Threats & Vulnerabilities
- Practices
- Security Requirements

Technology View
- Technology Vulnerabilities

Risk Analysis

Risks
Protection Strategy

October 2000
Management Practice Categories

General Management

Policy

Personnel

Security Program Management

Physical Security

Contingency Planning/Disaster Recovery
Technology Practice Categories

- System and Network Management
- Incident Management
- Encryption
- Authentication and Authorization
- Monitoring and Auditing
SEI Risk Assessment Resource

- Will be available freely over the Web
- Derivative products encouraged
- SEI will provide training courses
- Will have been validated in field
- Expected to be available 6-12 months
HIPAA Security Summit
Implementation Guidelines

Roger May
Support

- Johns Hopkins
- WEDI / Jim Schuping and Steve Lazarus
- Track Leaders
- Executive Committee
- Sponsors
  - IBM, TRW, COMPAQ, KSM Healthcare Resources, Johns Hopkins, Microsoft, SMS
- Attendees
What Kind of Guidance?

- **Reasonable**
  - Can you live with it? Does it protect enough?
- **“Implementable”**
  - Can you put it into operation? Keep it there?
- **Scalable**
  - Dentists to Integrated Delivery Systems
- **Business Oriented**
  - How Do I fit it within my Business Processes?
- **Where to Start??**
Partners....

- CPRI
- D.O.D. Rainbow Series
- ASC X12N
- Consulting and Technology Firms
  - Best Practices
  - Other Industries
- Business Continuity Firms / Experts
- Then, We Synthesize
October 11 - 13, 1999
Baltimore

• Overview of HIPAA & Security Drill Down
• Reviewed Goals, Objectives, Methodology
  – Gathered Issues/Concerns to Address
  – What are you worried about?
• Broke Into Tracks
  • Business Impact Analysis, Solution Design, Implementations, Monitoring and Reporting
  • Led by “Volunteers”
  • “Vendor-isms” were discouraged
• Report Back Progress
  – Ask, Refine, Encourage, Torture, Other
• Repeat Steps Above
• Close and Go to Next Phase
3 Breakout Groups

- Business Impact Analysis
- Solution Design and Analysis
- Monitoring and Reporting

- Approach
- Content
### Who Contributed?

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payers</td>
<td>23</td>
</tr>
<tr>
<td>Providers</td>
<td>39</td>
</tr>
<tr>
<td>Consultants</td>
<td>47</td>
</tr>
<tr>
<td>Technology</td>
<td>22</td>
</tr>
<tr>
<td>Clearinghouses</td>
<td>4</td>
</tr>
<tr>
<td>Payer Vendors</td>
<td>3</td>
</tr>
<tr>
<td>Provider Vendors</td>
<td>10</td>
</tr>
<tr>
<td>Government</td>
<td>10</td>
</tr>
<tr>
<td>Professional Organizations</td>
<td>10</td>
</tr>
<tr>
<td>Law Firms</td>
<td>2</td>
</tr>
</tbody>
</table>
Assets We Took Into Summit

• Highly Refined Raw Material
  – By Track
  – Refined Matrix
  – Toolkit and Tools
  – Document Format (Logical Sequence)

• Volunteers to Create Finished Product

• Web-sites and Communications

• A Process

• A Timeline

October 2000
**So, Where Are We Now?**

- Executing the Plan
  - Drafting/Revising Guideline Document
- Maintaining Focus
- Receiving Very Positive Feedback
- Reviewers & Validations
  - Where you come in
- Roll-out Following Final Rules
- Looking for Greater Collaboration
  - CPRI-HOST
Going Forward

- Coordinate and Proliferate (with Your Help)
- Refine and Improve
  - Your / Our Guidance (Leverage Experience)
- Additional Thoughts? Send w/ Subject to:
  - hipaa.issues@smed.com
- Remain Coordinated w/ NPRM Timing
- Stay Tuned for Updates and Deliverables at
  
  www.smed.com/hipaa
  
  www.wedi.org
Thank you!