



HIPAA Security Rule Toolkit Project

E X E T E R

9841 Washingtonian Boulevard, Suite 400
Gaithersburg, Maryland 20878

Prepared for:
NIST's 7th Annual IT
Security Automation
Conference

...Easy to do Business With

About Exeter

Exeter is a privately held Veteran-owned Small Business led by an executive team with an extensive track record of achievement in government and the private sector. This experience has led to numerous client successes that are directly attributable to our proven proprietary methodologies and service delivery excellence.

The company embodies the positive aspects of small business: small enough to allow direct client and employee access to management, yet large enough to meet our commitments and address all client needs.

HIPAA Security Rule Toolkit Project Agenda

- Toolkit Overview
- Toolkit Project
- Content Development
- Security Automation
- Screen Shots
- Additional Information

Toolkit Overview

The purpose of this toolkit project is to help organizations ...

- better understand the requirements of the HIPAA Security Rule (HSR)
- implement those requirements
- assess those implementations in their operational environments

Toolkit Overview

Exeter's role

- Exeter is under contract with NIST to develop the toolkit application
- HSR Toolkit end product will be a freely distributable NIST product

Toolkit Overview

HIPAA Security Rule
establishes national
standards for a covered
entity to protect individuals'
electronic protected health
information (ephi)



Toolkit Overview

covered entity:

- Health Plans
- Health Plan Clearing Houses
- Health Care Providers

ephi:

•individually identifiable health information that is transmitted or maintained by electronic media



Toolkit Overview

Who?

From nationwide health plan providers with *vast resources ...*



... to small business & provider practices: limited access to IT expertise

What?

42 implementation specifications covering...

- Basic practices
- Security failures
- Risk management
- Personnel issues

How?

It depends...

on the size and scale of your organization

Toolkit Project

What it is ...



- A self-contained, OS-independent application to support various environments (hardware/OS)
- Support for security content that other organizations can reuse over and over
- A useful resource among a set of tools and processes that an organization may use to assist in reviewing their HSR risk profile

Toolkit Project

What it is not ...



- It is NOT a tool that produces a statement of compliance
 - NIST is not a regulatory or enforcement authority
 - Compliance is the responsibility of the covered entity

Content Development

The source of information was the HIPAA Security Rule, including NIST SPs:

- 800-66
- 800-53
- 800-53A
- HITECH Act

Content Development

Distilled the Security Rule to include not just questions but activities to assist in the implementation of requirements

§ HIPAA Security Rule

Maps

Specific Question
to Address Rule



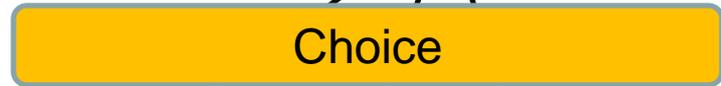
Content Development

§164.308(a)(3)(A)
Authorization and/or supervision (Addressable).

Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.



Question: HSR.A53
 Has your organization established chains or command and lines of authority for work force security?



Yes: If yes – do you have an organizational chart?

No: If no – provide explanation text

N/A: Not Applicable

Content Development

The result (so far) of this effort has been ...

- A set of over 1,000 unique questions
An Enterprise and Standard set
- With dependency and parent-child relationship mappings
- Covering all Safeguards including:
Administrative, Physical, Technical, Organizational, Policy & Procedures

Security Automation

Utilizing standards-based automation specifications such as OCIL allows:

- Ability to define questions (of type Boolean, Choice, Numeric, or String)
- Ability to define possible answers to a question from which the user can choose
- Ability to define actions to be taken resulting from a user's answer
- Ability to enumerate the result set

Security Automation

Benefits:

- Existing commercial tools that process SCAP can use the content (not locked down)
- Provides consistent and repeatable processes

Security Automation

Why OCIL?

- NIST endorsed standard
- OCIL is a portion of the Security Content Automation Protocol
 - Ask computer questions (OVAL)
 - Ask human questions (OCIL)
- This application is a clear intersection of security and automation

Security Automation

Why OCIL?

- Enabled data collection and SCAP conformance
 - *supports multiple authors*
- Answer logic
 - *can skip questionnaires based on answers*
 - *not implemented per UAT findings*
- Artifact assignment

The current specification of OCIL solved most of our needs except for a few...

Security Automation

Limitations Encountered

- No place to record an *organizational* target of the survey
- No method to indicate type of artifact required
 - *Necessary to implement business rules*
- No method to “*tag*” questions with an arbitrary value

So we developed a few extensions...

Security Automation

HSR OCIL Extensions

- Added “organization” as target for survey
- Added “type” attribute to artifact element
 - *To satisfy question condition (attachment, text)*
- Added “tag” attribute to test action result element
 - *Request from UAT to categorize questions*

Screen Shots

The screenshot displays a 'Profile Manager' window with the following fields and controls:

- Profile:** A dropdown menu showing 'Davis Memorial Medical Center' and a 'Change Name' button.
- Assessment Subject:**
 - Subject:** Text field containing 'The Davis Memorial Medical Center'.
 - Type:** Text field containing 'Hospital'.
 - Scope:** Text field containing 'Entire Hospital Records'.
 - Description:** Text area containing 'An evaluation of all medical records and data recorded for patients of the medical center will be evaluated.'
- Assessor:**
 - First Name:** Text field containing 'Mary'.
 - Last Name:** Text field containing 'Smith'.
 - Location:** Text field containing '1413 Medical Center Drive, Anytown, MD 25555'.
 - Phone:** Text field containing '301-555-1245'.
 - E-Mail:** Text field containing 'msmith@DMMC.org'.

At the bottom of the window, there are six buttons: 'Save', 'Save As...', 'Clear', 'Delete', 'Use Selected', and 'Close'.

Screen Shots

The screenshot shows a web-based application window titled "Questionnaire: HSRTK_Davis_Memorial_Medical_Center_110830_022812.xml". The interface includes a menu bar with "File", "Reports", "Tools", and "Help". The main content area is titled "Questionnaire: HIPAA Security Rule Toolkit Checklist" and "Profile: Davis Memorial Medical Center". A "Survey Dashboard" is displayed, showing a list of categories and their respective question counts and answer status:

Category	Questions	Answered	Status
164.308 ADMINISTRATIVE SAFEGUARDS	430	0	First unanswered question...
164.310 PHYSICAL SAFEGUARDS	146	0	First unanswered question...
164.312 TECHNICAL SAFEGUARDS	177	0	First unanswered question...
164.314 ORGANIZATIONAL REQUIREMENTS	35	0	First unanswered question...
164.316 POLICES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS	18	0	First unanswered question...

At the bottom of the dashboard, there are navigation arrows and a "Clear" button. The status bar at the bottom of the window indicates "0 out of 806 answered" and includes "Save" and "Exit" buttons.

Screen Shots

File Reports Tools Help

Questionnaire: HIPAA Security Rule Toolkit Checklist Profile: jp

164.308 ADMINISTRATIVE SAFEGUARDS

- 164.308(a)(1)(i) Standard: Security management practices
 - Has your organization developed, disseminated, reviewed/updated, and trained on your Risk Assessment policies and procedures?
 - Does your organization's risk assessment policy and procedures include the following:
 - Has your organization disseminated your Risk Assessment policy and procedures to all employees?
 - Has your organization disseminated its Risk Assessment policy and procedures to all contractors and vendors?
 - Has your organization defined the frequency of your Risk Assessment?
 - Has your organization reviewed and updated your Risk Assessment policy and procedures?
 - Has your organization identified the types of information systems that are in use?
 - Has your organization identified all information systems that are in use?
 - Does your organization inventory include all hardware and software for which you are responsible?
 - Has your organization analyzed its business functions and processes to identify information systems that are critical to the organization's operations?
 - Are all the hardware and software for which you are responsible inventoried?
 - Has your organization identified all hardware and software for which you are responsible?
 - Does your organization's inventory include removable media?
 - Is the current information system configuration documented?
- 164.308(a)(1)(ii) Implementation specifications:
 - Has your organization identified all the ePHI with which it is associated?
 - Has your organization considered all processes that create, receive, maintain, use, or disseminate ePHI?
 - Has your organization identified your external service providers?
 - Has your organization identified all human, natural, or environmental threats to ePHI that are reasonably likely to result in unauthorized access, use, disclosure, modification, destruction, or interference with the availability of any ePHI?
 - Has your organization conducted an assessment of the risks to ePHI that are reasonably likely to result from the identified threats?
 - Has your organization documented your risk assessment?
 - Has your organization periodically reviewed your risk assessment?
 - Has your organization periodically updated your risk assessment?

Question Text

Has your organization developed, disseminated, reviewed/updated, and trained on your Risk Assessment policies and procedures?

Instructions:
 --If yes, select Yes below and please attach your policy and procedure currently in use and please include your review/update schedule and training schedule.
 --If no, select No below.

References

SP 800-53 RA-1 Risk Assessment Policy and Procedures

Yes No
 Not Applicable

Attachments

Referenced Document	Attached	
		Add
		Remove

Comments

Flag Level: -- ▾

Clear

1 out of 14 answered

Save Exit

Screen Shots

164.308 ADMINISTRATIVE SAFEGUARDS

- 164.308(a)(1)(i) Standard: Security management p
- Has your organization developed, disseminated
- Does your organization's risk assessment polic
- Has your organization disseminated your Risk A

Question Text

Has your organization developed, disseminated, reviewed/updated, and trained on your Risk Assessment policies and procedures?

Instructions:
--If yes, select Yes below and please attach your policy and procedure currently in use and please include your review/update schedule and training schedule.

References

SP 800-53 RA-1 Risk Assessment Policy and Procedures

Yes No

Not Applicable

Flag Level: **1**

Toolkit Project

What it is ...again



- Support for security content that other organizations can reuse over and over
- Large organizations can develop/distribute internally
- Easily adapted to other domains

Additional Information

- Project has been in partnership with
 - G2 Inc
 - ThreatGuard Inc
 - Sue Miller J.D.

Partner entities that are assisting in defining functionality and usability:

- A state Medicaid Office
- A specialty clearinghouse
- A community hospital
- A non-profit regional hospital

Additional Information



Anticipated delivery is
December 2011

JP Chalpin

jchalpin@exeter.com