HIPAA Security Rule Toolkit Project

Prepared for:

NIST's 7th Annual IT Security Automation Conference

EXETER

9841 Washingtonian Boulevard, Suite 400

Gaithersburg, Maryland 20878

…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

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.

Maps

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

Choice

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

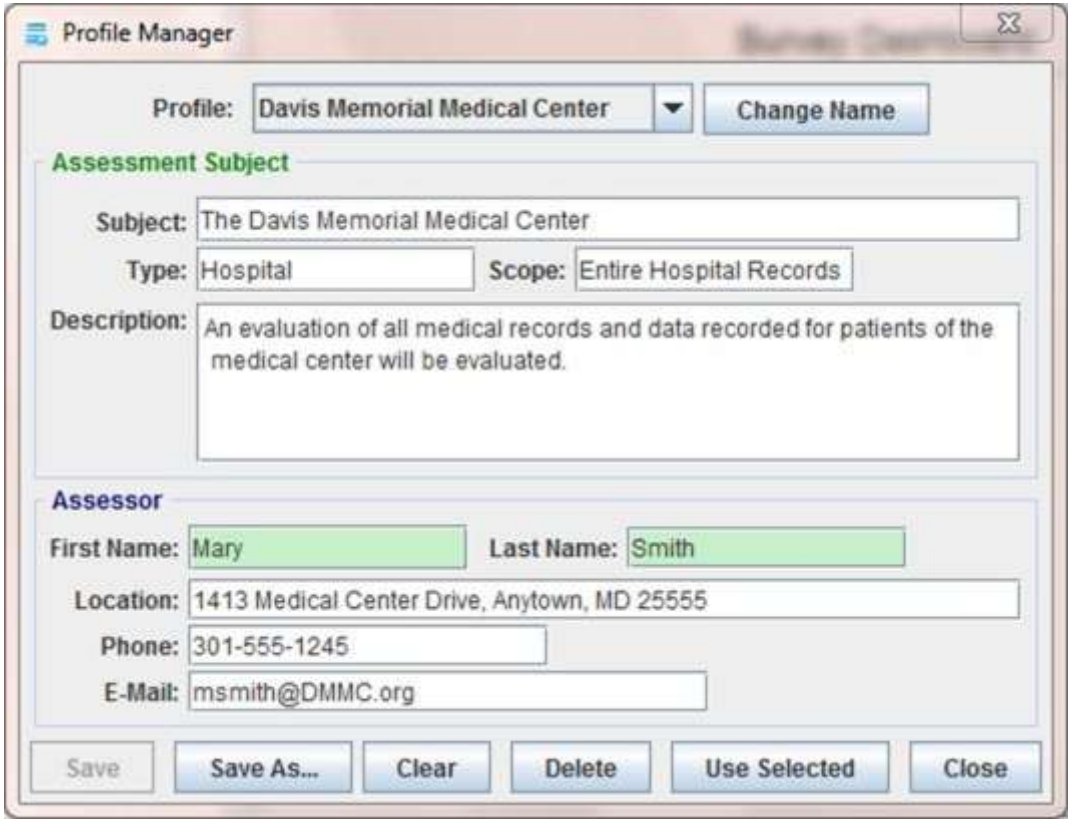
So we developed a few extensions…

Security Automation

HSR OCIL Extensions

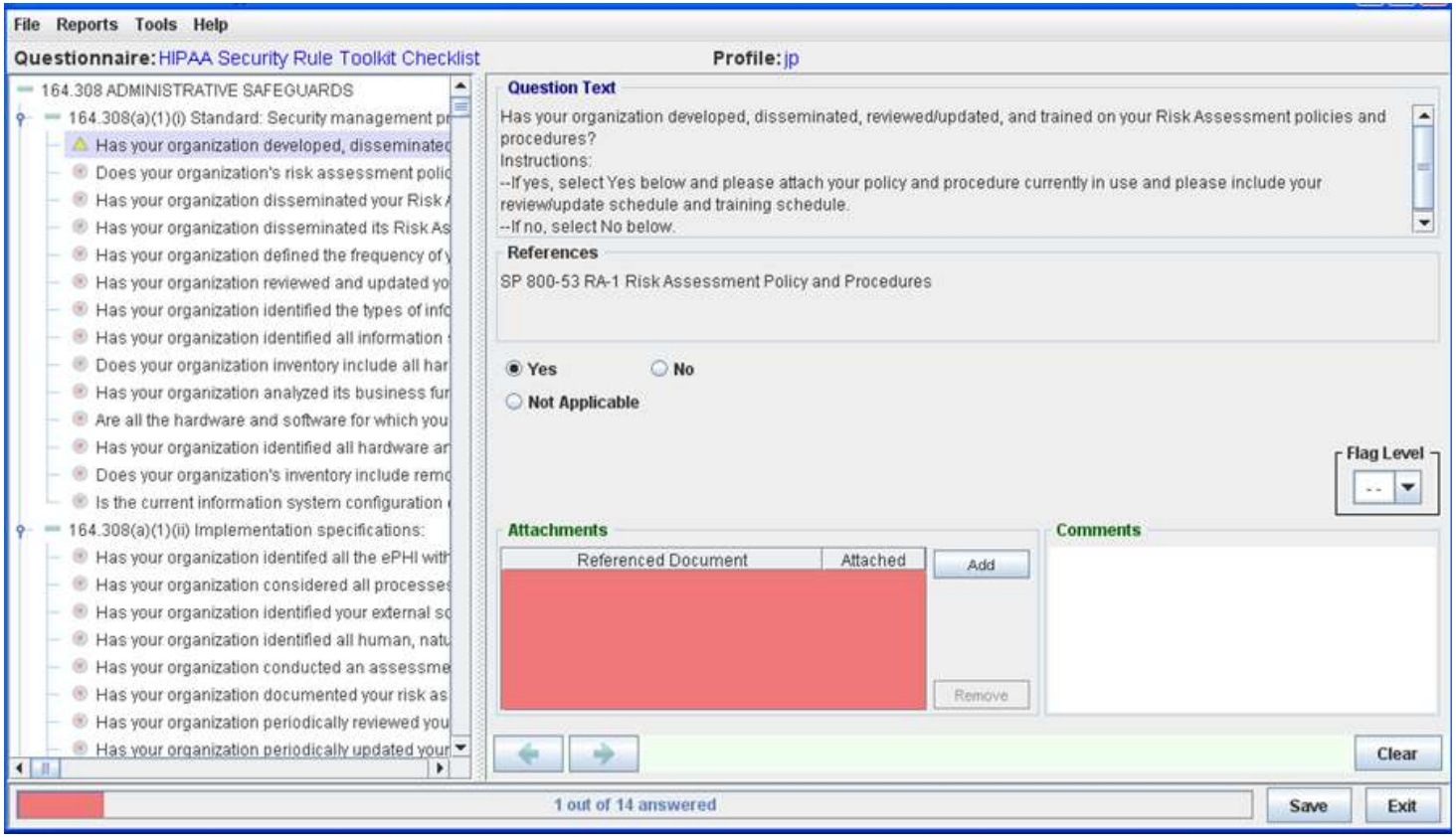
- Added “organization” as target for survey
- Added “type” attribute to artifact element
  - *To satisfy question condition (attachment, text)*
- Added “tag” attribute to *test_action_result* element
  - *Request from UAT to categorize questions*

Screen Shots

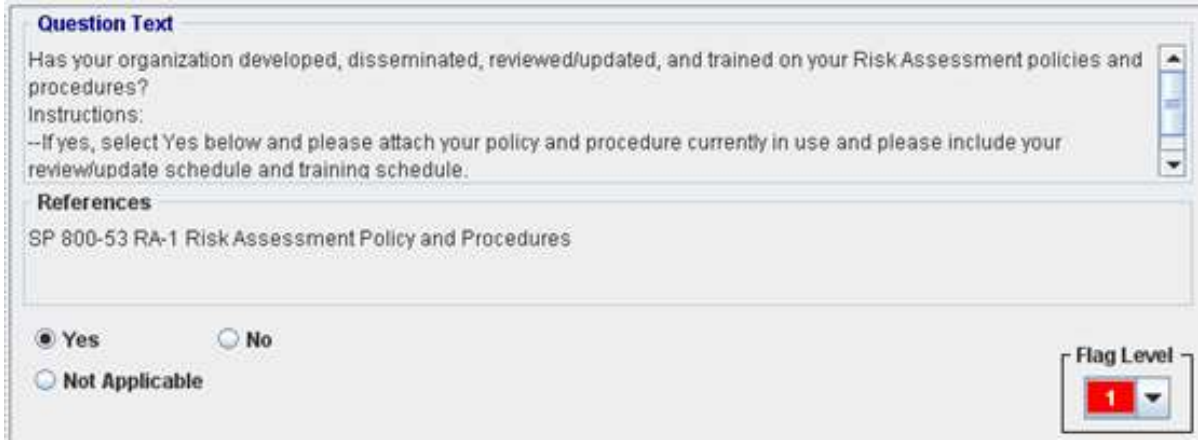


Screen Shots

Screen Shots



Screen Shots



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