HIPAA Security Rule Toolkit Project

Prepared for:

Safeguarding Health Information Conference

E X E T E R

9841 Washingtonian Boulevard, Suite 400

Gaithersburg, Maryland 20878

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
- The Toolkit Application
- 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

HSR establishes national standards for a *covered entity* to protect individuals' *electronic personal 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

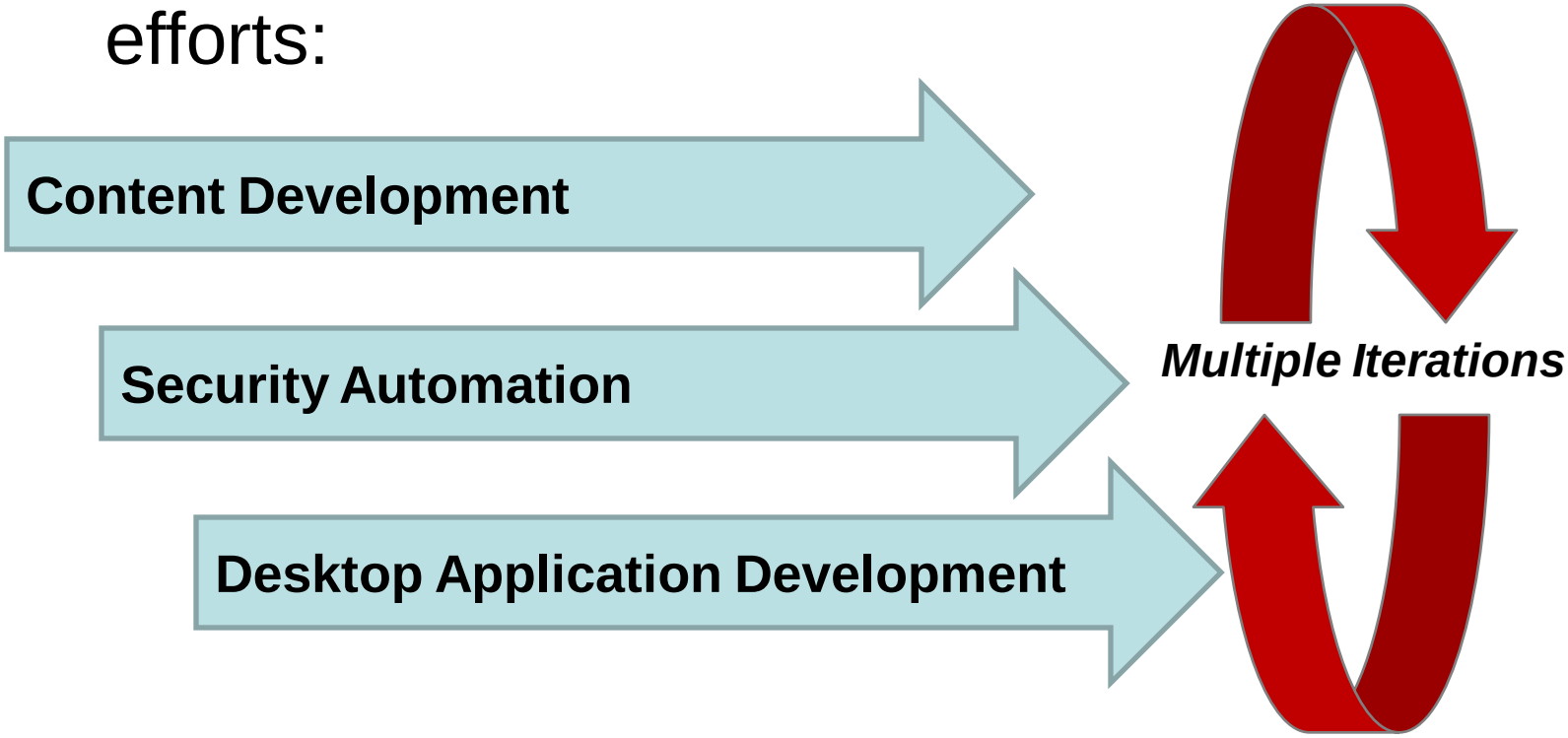
Toolkit Project

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

Toolkit Project

The Toolkit project consists of three parallel efforts:



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 of command and lines of authority for work force security?

Boolean

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

No: If no – provide explanation text

Content Development

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

- A set of over 1,000 unique questions
- With dependency and parent-child relationship mappings
- Covering all Safeguards including:

  Administrative, Physical, Technical, Organizational, Policy & Procedures, Breach Notification

Content Development

The resultant database categorizes and maps questions by:

- Policy: *Safeguard, Standard Specification, Special Publication Reference location*
- Unique ID
- English translation from “Legal-ese”

Content Development

164.308(a)(3)(B) Workforce clearance procedure (Addressable). Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Your organization needs to implement procedures to determine that access of one of your staff, employees, or workforce members to ePHI is appropriate, and meets the policies and procedures outlined above.	**SP 800-66 4.3.4 Establish a Workforce Clearance Procedure**	**9**	HSR.A63	Does your organization have a process and strategy that supports your organization's authorizes who are permitted to designate and grant access to ePHI? **This implementation specification is addressable**	**Y, $$, answer the remainder of the questions in this section**	**N, $%, outline what you do within your organization in the space below**	2 + 3	HSR.A63
		SP 800-66 4.3.4 Establish a Workforce Clearance Procedure	**7**	HSR.A64	Does your organization check an applicant's employment and educational references, if this is reasonable for such a job description?	**Y**	**N, if no explain**	2 + 3	HSR.A64
		SP 800-66 4.3.4 Establish a Workforce Clearance Procedure	**8**	HSR.A65	Does your organization do background checks, such as a Criminal Offender Record Information (CORI) check, if appropriate in the circumstances?	**Y, if yes name what checks performed**	**N, if no explain**	2 + 3	HSR.A65
		SP 800-66 4.3.4 Establish a Workforce Clearance Procedure	**10**	HSR.A66	Does your organization have formal and documented procedures for obtaining the necessary and appropriate sign-offs within your organizational structure to both grant and terminate access to ePHI?	**Y, if yes attach**	**N, if no explain**	2 + 3	HSR.A52
		SP 800-53 PS-2 Position Categorization	**1**	**HSR.A66(b)**	**Does your organization:**				**HSR.A66(b)**
		SP 800-53 PS-2 Position Categorization	**2**	**HSR.A66(c)**	1) assign a risk designation to all positions?	**Y**	**N, if no explain**	2 + 3	**HSR.A66(b)**
		SP 800-53 PS-2 Position Categorization	**3**	**HSR.A66(d)**	2) establish screening criteria for individuals filling these positions?	**Y**	**N, if no explain**	2 + 3	**HSR.A66(b)**
		SP 800-53 PS-2 Position Categorization	**4**	**HSR.A66(e)**	3) periodically review and revise positions risk designations? **Y/N, if yes name period, if no explain**	**Y, if yes name period**	**N, if no explain**	2 + 3	**HSR.A66(b)**
		SP 800-53 PS-3 Personnel Screening	**5**	**HSR.A66(f)**	Does your organization screen individuals prior to authorizing access to the information system?	**Y**	**N, if no explain**	2 + 3	**HSR.A66(f)**

Security Automation

Utilizing standards-based automation specifications – such as XCCDF, OVAL, OCIL – to implement those questions into a toolkit application that is “loosely coupled”

Security Automation

Benefits:

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

The Toolkit Application

Demonstration

Additional Information

- A comprehensive User Guide
- Examples of how to use and operate the Toolkit

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

Additional Information