



Connecting Healthcare ®



**Susan A. Miller, JD**

**NIST HIPAA Security Toolkit**

**HIPAA Summit Presentation Discussion**

# AGENDA

- What is the Toolkit
- A drive around the Toolkit
- HIPAA Security in 2013
- Clearinghouse Case Study
- Hospital Case Study
- Emerging Risk Analysis Focus Areas
- Toolkit next steps

# NIST HIPAA Toolkit

## ONLY HIPAA Security!

- Outline = HIPAA Security Rule
- Questions = NIST SP 800-66 & SP 800-53
- User Guide
- Download from NIST at <http://scap.nist.gov/hipaa/>
  - Microsoft Windows
  - Red Hat Enterprise Linux
  - Apple MAC OS
- Both Standard + Enterprise Versions

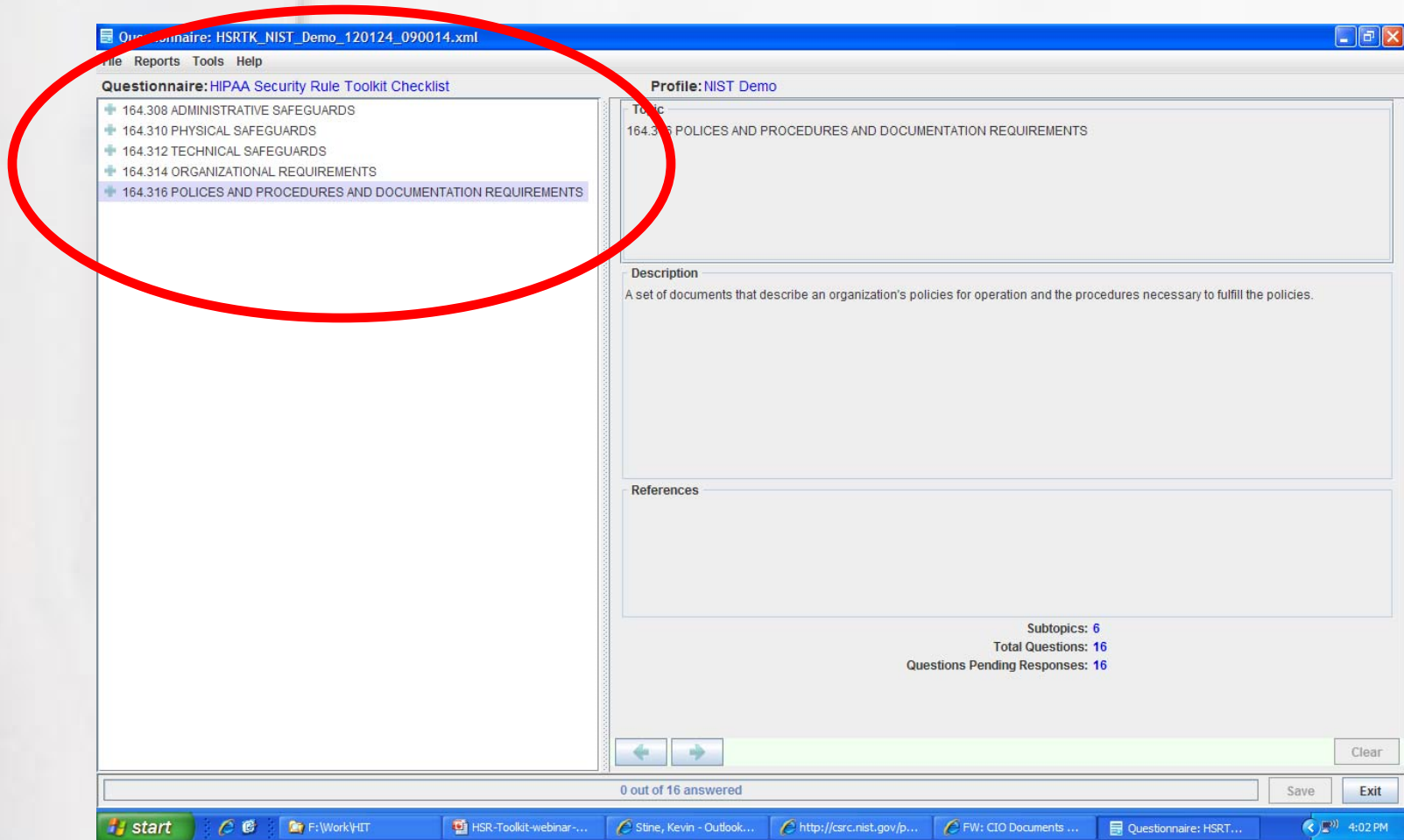
# Create a Profile

The screenshot displays the HSR Toolkit application window. The main interface is titled "Survey Dashboard" and shows a "Profile: --" dropdown. A "Questionnaire: --" dropdown is visible on the left. A "Profile Manager" dialog box is open, allowing the user to create or edit a profile. The dialog box contains the following fields and buttons:

- Profile:** A dropdown menu showing "NIST Demo" and a "Change Name" button.
- Assessment Subject:**
  - Subject:** A text field containing "NIST - Demo".
  - Type:** A dropdown menu showing "Covered Entity".
  - Scope:** A text field containing "System ABC".
  - Description:** A large text area containing "NIST demo February 2012".
- Assessor:**
  - First Name:** A text field containing "John".
  - Last Name:** A text field containing "Doe".
  - Location:** A text field.
  - Phone:** A text field.
  - E-Mail:** A text field.
- Buttons:** "Save", "Save As...", "Clear", "Delete", and "Close".

At the bottom of the main window, there is a status bar with a "[READ ONLY]" label, a "Save" button, and an "Exit" button. The Windows taskbar at the bottom shows the Start button, several open applications (F:\Work\Presentations, HSR-Toolkit-webinar..., HSR Toolkit), and the system clock showing 8:59 PM.

# Organized by Safeguard Family



# Explore the Application Interface

The screenshot displays the 'Questionnaire: HIPAA Security Rule Toolkit Checklist' application. The interface is divided into several sections:

- Navigation Menu:** A tree view on the left side of the application window, listing various security rule categories and sub-items. A red arrow points to this menu.
- Selected Question:** The main content area on the right, displaying the text of the selected question. A red arrow points to this section.
- References:** A section below the question text, listing relevant documents or standards. A red arrow points to this section.
- Responses:** A section for providing answers to the question, including radio buttons for 'Yes', 'No', and 'Not Applicable'. A red arrow points to this section.
- Flag Level:** A dropdown menu on the right side of the application, used to set the flag level for the question. A red arrow points to this dropdown.
- Attachments:** A table at the bottom left of the main content area, listing referenced documents and their attachment status. A red arrow points to this table.
- Comments:** A text area at the bottom right of the main content area, used for providing additional comments. A red arrow points to this text area.
- Progress Bar:** A horizontal bar at the bottom of the application window, showing the progress of the questionnaire. A red arrow points to this bar.

Red arrows are used throughout the image to highlight these specific components of the application interface.

# Generate Reports

Questionnaire: HSRTK\_NIST\_Demo\_120124\_090014.xml

File Reports Tools Help

Que HSR Safeguard Families Security Rule Toolkit Checklist Profile: NIST Demo

Flagged Items  
Uncommented Items  
All

Survey Dashboard

**HIPAA Security Rule Toolkit Checklist**  
Questions: 492  
Answered: 3  
Percent Completed: 0% [Jump to first unanswered question...](#)

**164.308 ADMINISTRATIVE SAFEGUARDS**  
Questions: 245  
Answered: 3  
Percent Completed: 1% [Jump to first unanswered question...](#)

**164.310 PHYSICAL SAFEGUARDS**  
Questions: 95  
Answered: 0  
Percent Completed: 0% [Jump to first unanswered question...](#)

**164.312 TECHNICAL SAFEGUARDS**  
Questions: 101  
Answered: 0  
Percent Completed: 0% [Jump to first unanswered question...](#)

**164.314 ORGANIZATIONAL REQUIREMENTS**  
Questions: 35  
Answered: 0  
Percent Completed: 0% [Jump to first unanswered question...](#)

**164.316 POLICES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS**  
Questions: 16  
Answered: 0  
Percent Completed: 0% [Jump to first unanswered question...](#)

3 out of 492 answered

Save Exit

start F:\Work\Presentations HSR-Toolkit-webinar-... Questionnaire: HSRTK... 9:02 PM



# The Value of the Toolkit

- Prompts consideration of risks
- Suggests safeguards/controls
- Provides documentation repository
- Go-to reference for audits
- **NIST “it is not a compliance tool!”**



# HIPAA Security in 2013

- Omnibus Final Rules
  - Combining
    - July 2010 NPRM on HITECH changes to HIPAA
    - October 2009 NPRM on GINA changes to HIPAA
    - August 2009 IFR on HIPAA Breach Notification
    - October 2009 IFR on HIPAA Enforcement Rule
  - Compliance Dates: 180 days from effective date (30-60 days)
- OCR audits
  - 15 Audits in 2011, only CEs
  - Audit Protocols 2012
  - 95 Audits in 2012, only CEs
  - Most likely CEs + BAs
- Meaningful Use Risk Analysis



# Culture of Compliance

- OCR aggressively enforcing the HIPAA Privacy, Breach and Security Rules
- OCR suggests that HIPAA covered entities (CEs) and business associates (BAs) should have a robust HIPAA Privacy and Security compliance program, including:
  - Employee Training
  - Vigilant implementation of policies and procedures
  - A prompt action plan to respond to incidents and breaches
  - Regular internal audits
- **All of this requires Management Commitment**

# National Clearinghouse Case Study

## Jopari Solutions, Inc.



- Jopari Solutions is an EDI technology solutions company as well as a national clearinghouse for the workers' compensation, auto insurance and healthcare industry
- EDI Transaction Sets (ASCX12) Include:
  - Medical Claims and Acknowledgments
  - Medical Reports/ Attachments
  - Electronic Remittance Advice
  - Electronic Fund Transfers
- Web Portal Service Solutions
- Healthcare Electronic Attachment Solutions
- Customers include Payers, Healthcare Providers, national clearinghouses, practice management system, banking and other technology vendors

# Manual HIPAA Security Risk Assessment Challenges

## Pre NIST Toolkit

### Pre Planning the NIST HIPAA Security Risk Assessment

- Security Team met 3 times a week for 2 hours /6 Weeks
- Pre audit data collection/ risk assessment interview/ survey questions
- Senior management buy in – major concern was time management of resources

### Process Documentation Challenges -Lacked automated documentations tools

### Challenge of Cross Referencing Multiple Documents / Other Security Compliance Requirement Considerations –very labor intensive process

### HSR Assessment & Report Generation Challenges – Communicate IT risk assessment to technical as well as the non technical audience

# Scope of HSR Assessment –Manual Process

- Excellent Support from Senior Management -Understood Compliance / Business Impact
- 12 Departments / groups of functions with 76 applications or groups of applications/Identified 35 Risk Issues
- Required cross walking other security requirements to the NIST HSR to mitigate redundant controls/ policies and procedures to ensure consistency
- Updated security policies , procedures and training program
- **Manual Process**= timely , costly , redundant processes and impacted IT resources company wide

# NIST HSR Assessment Toolkit

## How is it being used?

### Using the Enterprise version

–To Automate Previously Manual Tasks

- simplifies the process to identify, prioritize and communicate key IT risk and security metrics
- provides the ability to consolidate multiply reports to generate HSR analysis and management reports
- To Reduce IT Risk Assessment **Time and Expense**- Workflow Automation
- To increase effective IT risk assessment communication for the business audience
- NIST converted many of the legal / IT terminology question and reports into “English” which enable the security team to clearly communicate IT risks to non-technical audiences.

## Assessment Toolkit

### How is it being used?

#### Document Repository Tool

Provides flexibility and efficiency in metrics and reporting. Used as document repository to include links to security policy and procedures as they relate to specific security controls

#### Document Tool to Help Optimize Audit Results

Enables easy access for users and auditors to cross reference security controls against policies and procedures. Also provides tools to update security controls



# How is it working?

- Easy to implement and the application is flexible/menu driven
- Automated documentation and report generation tools are great and really save time as compared to manual processing
- The organization of the NIST HSR Assessment content , makes it easy to cross reference other security control requirements to mitigate redundant processes and also helps to standardize the use of language across supporting documentation
- Excellent ROI –Free Resource Tool  
**Projecting at least a 50 % reduction** in time and resource requirements for next NIST HSR Assessment

# Hospital Case Study



2<sup>nd</sup> largest hospital in Vermont

- Established September 6, 1896
- Number of Beds: 188
- Emergency Department Visits: 35,740
- Number of Births: 397
- Rehabilitation Visits (Physical, Occupational, Speech Therapy): 35,835
- Medical and Radiation Oncology Visits: 2,4290
- Outpatient Registrations: 154,918
- Inpatient Admissions: 7,022
- Financial Assistance: \$4,574,581
- Medical Staff: 234
- Medical Specialties: 40
- Employees: 1,530
- Volunteers: 379

# RRMC Security Compliance

- Good record of proactive risk analysis and remediation
- Dedicated, growing team dedicated to information security
- Most recent risk analysis examined 18 departments/groups of functions with 73 applications or groups of applications, and 116 identified risk issues
- Adopting a complete suite of security policies and procedures
- Did not have a prior documentation system for information security

# How is it being used?

- RPMC has already gone through multiple risk analyses and reviews
- Needed a way to organize the documentation
- Considered a Wiki or SharePoint intranet site; slow progress
- Using the HSR Toolkit to:
  - Review controls and look for issues
  - Organize the supporting documentation for compliance
  - Keep the documentation current and relevant

# Implementation Expectations vs. Reality

- Using the Enterprise version
- 2-person information security team:
  - One with an administrative security background
  - One with a technical security background
- Planned 2-hour meetings, 2 days a week, for 8 weeks
- Completed first pass in only 5 weeks
- Using flags to identify areas needing further development, references

# How is it working?

- Great way to organize documentation for compliance
- Asks about lots of controls
- Can use Comments field for justifications, explanations
- Asks about lots of controls they haven't implemented

# Incorporating the HSR Toolkit into Daily Operations at RRMCMC

- RRMCMC has XML development capability, considering adding questions and customizing for RRMCMC-specific controls
- ✓ Need to integrate HSR Toolkit review and updating into policy and procedure development and adoption processes
- ✓ Still developing the routines and processes, but sleeping better
- ✓ Overall, very happy to be using the HSR Toolkit



# Emerging Risk Analysis Focus Areas

- EHR Audit controls and process
- Emergency access (break the glass) controls
- Minimum necessary in the use of an EHR (enhanced role and permission controls)
- CE update its access/authorization/modification and termination procedures to accommodate a revised environment with the HER
- Review transport/transmission and related controls for:
  - CCD and other types of exchange
  - HIE connectivity
  - Immunization registry connectivity
  - PQRS or related connectivity
  - Other public health connectivity (syndromic surveillance/lab data)
  - Patient portals

# Tools

Tools may create tribulations

- Seeing many “tools” being produced and sold or promoted
- A checklist IS NOT A RISK ANALYSIS!!!!!!
- REC checklists
- Other checklists
- EHR vendor solutions
- Incomplete Risk Analyses reports

# NIST HIPAA Toolkit: Next Steps

- Omnibus Rules update of content
- 2013 tech revisions
- Additional reports planned
- Just being planning now
  - Will know more later in 2013

# Questions?

[TMSAM@aol.com](mailto:TMSAM@aol.com)

Office: (978) 369-2092

Mobile: (978) 505-5660

# THANK YOU!