NIST HIPAA Toolkit
CASE STUDIES

June 7, 2012

Presenters

- Susan A. Miller, JD, Moderator
- Sherry Wilson, E-VP, Jopari Solutions
- Jim Sheldon-Dean, Lewis Creek Systems, LLC

AGENDA

- What is the toolkit, and where can you find it?
- The toolkit value
- Case Study: National Clearinghouse
- Case Study: Hospital
- Case Study: Specialty Clearinghouse

NIST HIPAA Toolkit

ONLY HIPAA Security!

- 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

The Value of the Toolkit

- Prompts consideration of risks
- Suggests safeguards/controls
- Provides documentation repository
- Go-to reference for audits

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 HSR 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

Jopari Solution Inc :
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.

NIST HSR 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 <u>at least a 50 % reduction</u> in time and resource requirements for next NIST HSR Assessment.

How is it not working?
Opportunities for Enhancements

- **“Assess Once, Comply with Many”**
  Provide tools to help identify and eliminate overlapping control requirements that result from multiple standards and regulatory requirements

- **Project Remediation Tracking to Improve Security Control Deficiencies**
  Allow assignment and status tracking of remediation projects. Projects could be tracked according to ownership and deadlines and updated in the document repository.

- **Automated Alert Notification to Ensure Current Assessment Information**
  Automatically detect when information compliance dates have expired and need to be updated to keep compliance and risk metrics up-to-date

- **Automate Survey Workflow**
  Provide an enhance mechanism for identifying, capturing an automating business stakeholder input into the risk analysis process

Hospital Case Study

Rutland Regional Medical Center

An Affiliate of Rutland Regional Health Services

2nd 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?

- RRMC 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? How is it not 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
- “Do we need to say ‘yes’ to everything?”
- Lawyerly language can be tiring
- Concerns about keeping references correct as policies and procedures change

Incorporating the HSR Toolkit into Daily Operations at RRMC

- RRMC has XML development capability, considering adding questions and customizing for RRMC-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

➢ Thanks to Patti Tamborini and Joshua Griffin at RRMC for sharing their experience!

Coastal Medical Billing– small covered entity Case Study

- Specialty Clearinghouse
  - EMT Billing only
  - EMTs mostly in municipal fire departments
  - ~ 65 municipalities as clients, most in MA, some in ME and VT
  - ~ 25 staff, 4 are remote staff

CMB Security Compliance

- Full set of privacy and security policies and procedures
  - First drafted in 2002, and 2003
  - Added breach (2010) and state ‘red flags’ (2011) polices and procedures

- Security audit in 2004 + 2005 (full risk analysis with to do list), 2007 (re-write the contingency plan), 2012 (full risk analysis using NIST HIPAA Security toolkit, on-going)

- Security training initially in 2003, and
  - each year there after

CMB Security Compliance

- CMB HIPAA Team
  - Privacy officer
  - Security officer
  - 2nd System administrator
  - System administrator – outsourced
  - HIPAA attorney – outsourced

Toolkit Implementation

- Standard Toolkit
  - Face-to-face meetings once a week
    - began 3/26/2012
      - In attendance security officer, system administrator, HIPAA attorney
      - Converted toolkit questions o module word documents, one for each security area, recorded all answers and issues on the work documents
    - Middle of May 2012 changed to phone calls, 2 – 3 times a week
- CMB's policy and procedure manual being updated simultaneously
- Next level CMB training being planned
- Will add HIPAA privacy, and breach, plus state identity theft assessment and audit

What works – what does not work!

- Converting the questions into modular word tables helped
  - Creating a 2012 base line
- Like that the controls are part of the questions
- Needed lots of hand holding to get started
  - Many terms and concepts need to be explained
  - Resorting some of the questions, specifically in the contingency planning areas
- NIST HIPAA Security Toolkit, as made into modular word documents will be used for the 2013 HIPAA self assessment and audit

QUESTIONS?

NIST HSR ASSESSMENT TOOLKIT

Special thank you to NIST and everyone that worked on the toolkit. It a great tool and has really made a difference in how we approach the HSR Assessment process through workflow automation.

Contact Information:

Sherry Wilson , EVP and Chief Compliance Officer
Jopari Solutions, Inc.
Email: sherry_wilson@jopari.com
Phone: 925 459 5218
www.jopari.com

Contact Information

- **Sue Miller**
  - TMSAM@aol.com
  - 978-369-2092
- Sherry Wilson
  - sherry_wilson@jopari.com
  - 925 459 5218
- Jim Sheldon-Dean
  - jim@lewiscreeksystems.com
  - 802-425-3839