March 31, 2016
12pm EST
Presented by the ISSA Healthcare SIG

Existing Tools and Frameworks for Securing the Healthcare Industry

Agenda

- Presenter Introduction & Webinar Contributors
- ISSA & Healthcare SIG Overview
- Quick Case Study: Ransomware
- Guiding Principals of Information Systems Security
- HIPAA/HITECH Rule Highlights
- Tour Existing Tools and Resources
- Frameworks and Organizational Certifications
- Summary
- Questions

Agenda

- Presenter Introduction & Webinar Contributors
- ISSA & Healthcare SIG Overview
- Quick Case Study: Ransomware
- Guiding Principals of Information Systems Security
- HIPAA/HITECH Rule Highlights
- Tour Existing Tools and Resources
- Frameworks and Organizational Certifications
- Summary
- Questions

Presenter Introduction

Grant F. Johnson, CISSP, CISM
Information Technology Security Consultant
Array Information Technologies, Inc.
GJohnson@Array.net
517-337-1254

Healthcare SIG Webinar Contributors

Michael Brown, Manager/Sr Information Security Consultant
24By7Security, Inc.

Leah Lewis, Program Director
Information System Security Association

Dean Sorensen, Senior Security Consultant
Carosh Compliance Solutions

DISCLAIMER

This presentation is for educational purposes only and does not constitute professional or legal advice. Contents include opinions and interpretations of the authors and presenter.

Mission Statement

ISSA is a non-profit organization for the information security profession committed to promoting effective cyber security on a global basis.

a) Being a respected forum for networking and collaboration

b) Providing education and knowledge sharing at all career lifecycle stages

c) Being a highly regarded voice of information security that influences public opinion, government legislation, education and technology with objective expertise that supports sound decision-making"

FACTS

- Founded in 1984.
- 11,000 members from across the globe.
- 140 local chapters in 70 countries.
- Governed by a member elected Board of 13.

Healthcare Special Interest Group (SIG)

Vision: Establish and maintain collaborative models for information security within healthcare organizations.

Mission: Drive collaborative thought and knowledge-sharing for information security leaders within healthcare organizations.

- Must be an ISSA member to join; no additional cost or requirement.
- Over 200 members from across the globe.
- Secure website provides: Group Directory, Event Calendar, Blogs, Forums, and Photo Gallery.

Quick Case Study

Hollywood Presbyterian Medical Center (HPMC)
February 2016

- Event: A hacker, using a ransomware virus, seized control of the hospital's computer systems for approximately one week.
- Reported Contingency Operations:
  - Some patients transported to other hospitals
  - Returned to pen and paper for record-keeping
  - Fax machines for document exchange
- Virtually Limited Recovery Options:
  - Restore from backups
  - Pay Ransom (HPMC ended up paying ~$17,000)

Quick Case Study

Hollywood Presbyterian Medical Center (HPMC)
February 2016

- Questions…
  - Was malware protection present and up-to-date?
    - Host Intrusion Detection/Prevention
    - Network Intrusion Detection/Prevention
  - Were data backups available and current?
  - Was there a formal Contingency Plan in place?
  - Was there a formal Emergency Mode Operation Plan in place?

Guiding Principal of Information Systems Security

Over Arching Goal…

The primary goal of Information Systems Security is to reduce risk to an acceptable level.

Considerations…

- **Compliance Requirements**
- **Organizational Risk Tolerance (appetite)**
- **Contractual Requirements**
- **Value of data and systems relative to C-I-A**

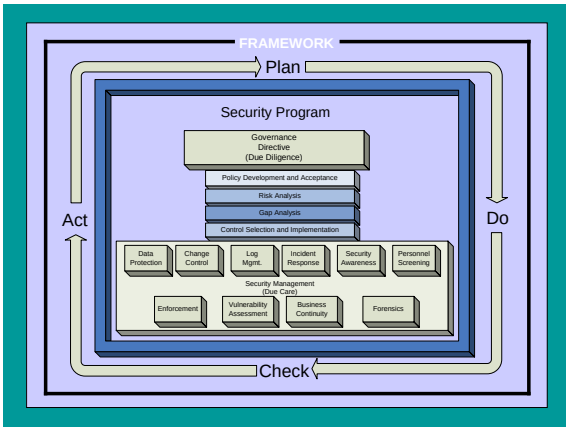
Guiding Principal of Information Systems Security

Over Arching Goal…

The primary goal of Information Systems Security is to reduce risk to an acceptable level.

Considerations…

- ❑ **Compliance Requirements**
- ❑ **Organizational Risk Tolerance (appetite)**
- ❑ **Contractual Requirements**
- ❑ **Value of data and systems relative to C-I-A**



HIPAA Background

HIPAA

Health Insurance Portability and Accountability Act

- ❑Federal Law enacted in 1996
- ❑Elements:
  - ❑Privacy Rule
  - ❑Transactions and Code Set Rule
  - ❑Security Rule
  - ❑Unique Identifier Rule (National Provide Identifier)
  - ❑Enforcement Rule

HIPAA Background

HIPAA

Health Insurance Portability and Accountability Act

- ❑Federal Law enacted in 1996
- ❑Elements:
  - ❑Privacy Rule
  - ❑Transactions and Code Set Rule
  - ❑Security Rule
  - ❑Unique Identifier Rule (National Provider Identifier)
  - ❑Enforcement Rule

Omnibus Final Rule Background

- ❑ Department of Health and Human Services (HHS) set rules for the statutory changes under the ***HITECH Act***, enacted as part of the American Recovery and Reinvestment Act of 2009

- ❑ Elements:
  - ❑ Meaningful Use - Advance Health Information Technology
  - ❑ Business Associates bound to HIPAA Compliance
  - ❑ Pro-Active Audits by the Office of Civil Rights (OCR)
  - ❑ New Breach Notification Requirements
  - ❑ Increased criminal and civil penalties

HIPAA Security Rule Guiding Statement

Covered Entities and Business Associates must maintain reasonable and appropriate Administrative, Technical, and Physical safeguards to ensure the Confidentiality, Integrity, and Availability (C-I-A) of electronic Protected Health Information (ePHI).

HIPAA Security Rule Guiding Statement

Covered Entities and Business Associates must maintain reasonable and appropriate Administrative, Technical, and Physical safeguards to ensure the Confidentiality, Integrity, and Availability (C-I-A) of electronic Protected Health Information (ePHI).

HIPAA Security Rule Guiding Statement

Covered Entities and Business Associates must maintain reasonable and appropriate Administrative, Technical, and Physical safeguards to ensure the Confidentiality, Integrity, and Availability (C-I-A) of electronic Protected Health Information (ePHI).

HIPAA Security Rule Guiding Statement

Covered Entities and Business Associates must maintain reasonable and appropriate Administrative, Technical, and Physical safeguards to ensure the Confidentiality, Integrity, and Availability (C-I-A) of electronic Protected Health Information (ePHI).

HIPAA Security Rule Guiding Statement

Covered Entities and Business Associates must maintain reasonable and appropriate Administrative, Technical, and Physical safeguards to ensure the Confidentiality, Integrity, and Availability (C-I-A) of electronic Protected Health Information (ePHI).

HIPAA Security Rule Guiding Statement

Covered Entities and Business Associates must maintain reasonable and appropriate Administrative, Technical, and Physical safeguards to ensure the Confidentiality, Integrity, and Availability (C-I-A) of electronic Protected Health Information (ePHI).

HIPAA/HITECH Security Rule Highlights

One Size Does Not Fit All

When a Covered Entity or Business Associate is deciding which security measures to use, the Security Rule does not dictate those measures, but requires the organization to consider:

- **Its size, complexity, and capabilities,**
- **Its technical, hardware, and software infrastructure,**
- **The costs of security measures, and**
- **The likelihood and possible impact of potential risks to ePHI.**

HIPAA/HITECH Security Rule Highlights

Organizational Requirements:

If a Covered Entity (CE) knows of an activity or practice of the Business Associate (BA) that constitutes a material breach or violation of the BA's obligation, the CE must take reasonable steps to cure the breach or end the violation. Violations include the failure to implement safeguards that reasonably and appropriately protect ePHI.

HIPAA

A risk analysis/assessment process includes, but is not limited to, the following activities:

- ❑ **Evaluate the likelihood and impact of potential risks to ePHI**
- ❑ **Implement appropriate security measures to address the risks identified in the risk analysis**
- ❑ **Document the chosen security measures and, where required, the rationale for adopting those measures, and**
- ❑ **Maintain continuous (on-going), reasonable and appropriate, security protections**

A Tour of Tools and Resources for HIPAA Security Management

Public/Government Supported:

- ❑ **U.S. Department of Health and Human Services (HHS.gov)**
- ❑ **U.S. Government Publishing Office (ECFR.gov)**
- ❑ **National Institute of Standards and Technology (NIST.gov)**
- ❑ **HealthIT.gov (in partnership with the National Learning Consortium)**

Privately Supported:

- ❑ **Google - Vendor Security Assessment Questionnaire (VSAQ)**
- ❑ **HITRUST Alliance**
- ❑ **International Organization for Standardization (ISO)**

A Tour of Tools and Resources for HIPAA Security Management

Public/Government Supported:

- ❑ **U.S. Department of Health and Human Services (HHS.gov)**
- ❑ **U.S. Government Publishing Office (ECFR.gov)**
- ❑ **National Institute of Standards and Technology (NIST.gov)**
- ❑ **HealthIT.gov (in partnership with the National Learning Consortium)**

Privately Supported:

- ❑ **Google - Vendor Security Assessment Questionnaire (VSAQ)**
- ❑ **HITRUST Alliance**
- ❑ **International Organization for Standardization (ISO)**

A Tour of Tools and Resources for HIPAA Security Management

U.S. Department of Health and Human Services (HHS)

Path: HHS Home (HHS.gov) > HIPAA > HIPAA for Professionals

- ❑ **"Go To" place for official HIPAA/HITECH Privacy and Security Rule information.**
- ❑ **Site does not contain tools (except one for healthcare providers).**

A Tour of Tools and Resources for HIPAA Security Management

U.S. Government Publishing Office
The Electronic Code of Federal Regulations (e-CFR)

Appendix A to Subpart C of Part 164

Security Standards: Matrix

Potential Use: A reference for mapping HIPAA Security Standards to the Implementation Specifications. Can be used as a "checklist", of sorts.

A Tour of Tools and Resources for HIPAA Security Management

National Institute of Standards and Technology (NIST)

Path: NIST Home (NIST.gov) > Information Technology Portal

- **NIST security specific documents:**
  - Managing Information Security Risk: Organization, Mission, and Information System View (800-39)
  - Framework for Improving Critical Infrastructure Cybersecurity (aka, NIST CSF)
  - NIST CSF – HIPAA Security Crosswalk
  - An Introductory Resource Guide for Implementing the HIPAA Security Rule (800-66-R1) [not updated since 2008]
  - Many others: http://csrc.nist.gov/publications/PubsSPs.html
- **NIST HIPAA Security Rule (HSR) Toolkit (downloadable)**

This publication places information security into the broader organizational context of achieving mission/business success. The objective is to:

- Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate *governance* structures for managing such risk;
- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

Framework for Improving Critical Infrastructure Cybersecurity

[aka, NIST CSF]

Version 1.0

National Institute of Standards and Technology

February 12, 2014

Critical Infrastructure Sectors
There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.
Healthcare is a Critical Infrastructure Sector

Building from those standards, guidelines, and practices, the Framework provides a common taxonomy and mechanism for organizations to:

1) Describe their current cybersecurity posture;
2) Describe their target state for cybersecurity;
3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4) Assess progress toward the target state;
5) Communicate among internal and external stakeholders about cybersecurity risk.

HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

INFORMATION SECURITY

October 2008

This document can support the compliance efforts of covered entities in many ways, including:

- Ensuring that each organization is selecting methods and controls which adequately and appropriately protect EPHI of which they are the steward;
- Informing the development of compliance strategies that are in concert with the size and structure of the entity;
- Providing guidelines on best practices for developing and implementing a Risk Management Program; and
- Creating appropriate documentation that demonstrates effective compliance with the HIPAA Security Rule.

Templates

Enterprise: For large organizations; 809 Questions

Standard: For smaller organizations; 492 Questions

A Tour of Tools and Resources for HIPAA Security Management

HealthIT.gov Dashboard

Path: HealthIT.gov Home (HealthIT.gov) > For Providers & Professionals > Privacy and Security [A little difficult to navigate to find all the nuggets]

- ❑ **The National Learning Consortium (NLC)**
- ❑ **HIPAA specific resources:**
  - ❑ Guide to Privacy and Security of Electronic Health Information
  - ❑ Information Security Policy Template
  - ❑ Mobile Device Privacy and Security Resources
  - ❑ Security Risk Assessment Resources
    - ❑ SRA Tool (downloadable application or standalone documents)
    - ❑ Video
- ❑ **Privacy & Security Training Games**
  - ❑ Cybersecure: Your Medical Practice
  - ❑ Cybersecure: Contingency Planning

ISSA

Chapter 6 35
Sample Seven-Step Approach for Implementing a Security Management Process 35
Introduction 35
How to Get Started on Security 35
Sample Seven-Step Approach for Implementing a Security Management Process 37
Step 1: Lead Your Culture, Select Your Team, and Learn 37
Step 2: Document Your Process, Findings, and Actions 40
Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis) 41
Step 4: Develop an Action Plan 43
Step 5: Manage and Mitigate Risks 46
Step 6: Attest for Meaningful Use Security-Related Objective 53
Step 7: Monitor, Audit, and Update Security on an Ongoing Basis 54
Chapter 7 56
Breach Notification, HIPAA Enforcement, and Other Laws and Requirements 56
Civil Penalties 56
Criminal Penalties 56
The Breach Notification Rule: What to Do If You Have a Breach 57
Risk Assessment Process for Breaches 58
Reporting Breaches 58
Investigation and Enforcement of Potential HIPAA Rules Violations 60
Penalties for Violations 60
Other Laws and Requirements 61

Instructions

The Information Security Policy Template that has been provided requires some areas to be filled in to ensure the policy is complete. Once completed, it is important that it is distributed to all staff members and enforced as stated. It may be necessary to make other adjustments as necessary based on the needs of your environment as well as other federal and state regulatory requirements.

Items highlighted in red within the template are required and items highlighted in yellow may require some adjustments based on your environment. Each highlighted item has a number afterwards which is referenced below to assist you in the completion of this policy template.

Number	Value	Description
1	Company Name/Logo	Company name or logo of organization
2	Last Revision Date	Last revision date of the Information Security Policy
3	Document Owner	Document owner of the policy. This is usually someone at an executive level.
4	Approval Date	Date that the policy has been officially approved
5	Effective Date	Effective date of the policy. This can be a different than the approved date if needed.
6	Company Name	Company/Practice name. No logo used for this particular part of the policy
7	Outside Agencies	List any outside agencies or organizations, if applicable, whose laws, mandates, directives, or regulations were included in the policy, i.e. CMS, OHRS, JWA, etc.

[Company Name or Logo]	Policy and Procedure
Title: IDENTIFICATION and AUTHENTICATION	P&P #: IS-1.2
Approval Date: [Date]	Review: Annual
Effective Date: [Date]	Information Technology (TY5888, TY5915, TY5918, TY5923)

3 Identification and Authentication

3.1 USER LOGON IDS

Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

All user logon IDs are audited at least twice yearly[7] and all inactive logon IDs are revoked. The Practice Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees and contractors, at which time logon IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3)[8] unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Practice systems or networks must have a completed and signed Network Access Form (Appendix D). This form must be signed by the supervisor or department head of each user requesting access.

Appendix E – Incident Response Tools

Tool	Attached Form/Worksheet	Description
Security Incident Report	Security_Incident Report-Confidential.doc	Security incident report utilized by the reporting employee or witness to an incident or potential incident.
Security Incident Investigation	Security_Incident Investigation-Confident	Security incident investigation report that that allows for further investigation of a potential incident upon receipt of the initial security incident report.
Security Incident Log	Security_Incident Log-Confidential.xls	Security incident log to ensure incidents are tracked for further analysis and follow-up.
Security Breach Assessment Tool	Security_Incident Breach Assessment Co	Privacy breach assessment tool which can assist in determining the severity of a breach.

Appendix H – Employee Hiring and Termination Checklist

Employee Hiring and Termination Checklist

Company:		Starting Date of Employment:	
Employee Name:		Ending Date of Employment:	
Type of Termination:			

System Name	System/Device Description (If applicable to system)	Unique Type	Access Granted?	Access Granted By:	Date Access to Device Revoked	Access Removed By:	Date Access to Device Removed
Facility	Physical Areas (IT, Building, and Set of Accessible Areas)						
Network	Desktop/ Mobile/Remote) Email, URL, etc.						
Email	Outlook, Google, AIM IT etc.						
Clinical Documentation	EMR Inputs and Applications						
Practice Management	Inputs and Applications						
Office Software	Product, Version, and Components (i.e. Microsoft Word, Excel, Outlook, etc.)						
Laptop/Tablet	Manufacturer and Model No.						
Clinical/Clinical Printer	Manufacturer and Model No.						
POS	Manufacturer and Model No.						
Paper Files	Manufacturer, Size and Designation						
Comments:							

Worksheet: Excel Version Attached


Privacy & Security
Your Mobile Device and Health Information Privacy and Security
Read and Learn
Watch and Learn


Security Risk Assessment
Security Risk Assessment Tool
What is the Security Risk Assessment Tool (SRA Tool)?

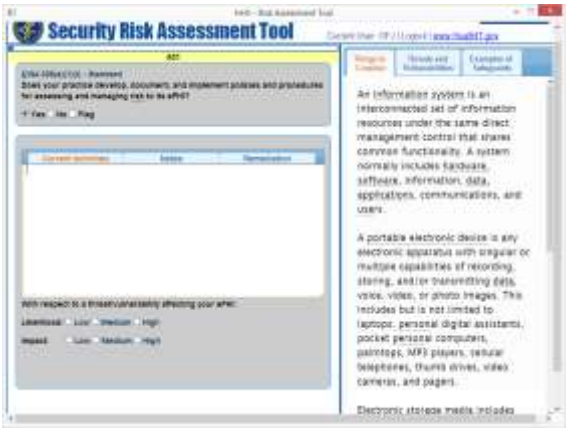

Security Risk Assessment Tool
Security Risk Assessments

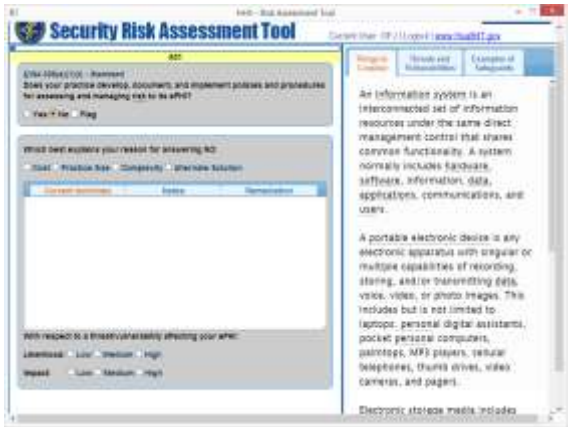

Security Risk Assessment Tool
Security Risk Assessments

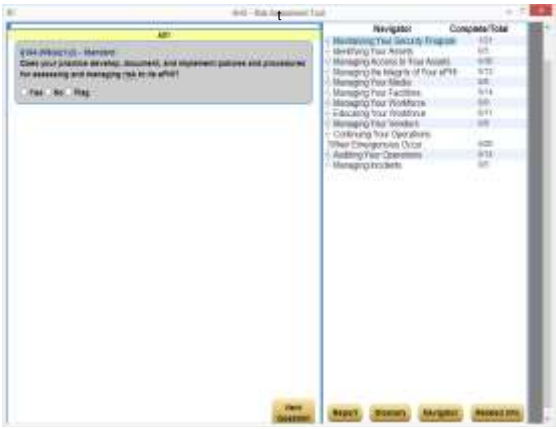

Security Risk Assessment Tool
Security Risk Assessments

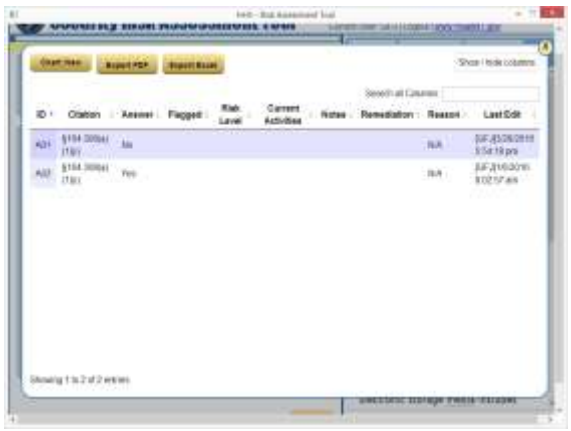

Security Risk Assessment Tool
Security Risk Assessments


Security Risk Assessment Tool
Tutorial
An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.
A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.


Security Risk Assessment Tool
An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.
A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.


Security Risk Assessment Tool
An information system is an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and users.
A portable electronic device is any electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers.






SRA Tool User Guide
User Guide

A Tour of Tools and Resources for HIPAA Security Management

Google - Vendor Security Assessment Questionnaires (VSAQ)

Path: https://vsaq-demo.withgoogle.com/

- A Web-based application released under an open-source license on GitHub.
- Assesses the security practices of suppliers (e.g., Business Associates), or to review and improve the organization's own security programs.
- A collection of four questionnaires that Google uses to review multiple aspects of a vendor's security:
  - Web application security
  - Infrastructure security
  - Physical and data center security
  - An organization's overall security and privacy program.
- Not HIPAA Specific

Private Frameworks and Certifications

Name	Non-Profit	Organizational Certification	Focus	No. of Controls/ "Domains"	Audited	Comments
HITRUST Alliance	Yes/No	CSF (previously called Common Security Framework)	Information Systems Security & Privacy (HIPAA focused)	149/14	Audited by HITRUST approved 3rd Party CSF Assessors	Published "Healthcare Sector Cybersecurity Implementation Guide" **Third Party Assurance Program**
International Organization for Standardization (ISO)	Yes – member organization funded	ISO/IEC 27001:2013	Information Security Management System (ISMS) program	114/14	Audited by approved 3rd Party	Internationally Recognized Standard

Value of Frameworks and Certifications

- **Framework:**
  - Provides Structure
  - Is a "Best Practice" for mature Information Systems Security Programs
  - Demonstrates "Due Care" and "Due Diligence"
  - A common language and format for information exchange between organizations.
- **Organization Certification:**
  - Tied to a specific Framework
  - Audit verification by external parties
  - Provides confidence
  - Some healthcare insurance payors are beginning to require certification of their Business Associates.

Webinar Summary

- Information Systems security is an on-going process that should be deliberately engrained in the organizational culture.
- HIPAA Security is complex and depends highly on the size, complexity, and capabilities of the organization; emphasis is on the application of "reasonable and appropriate" safeguards.
- There are many existing documents and tools that can help an organization build or streamline a mature HIPAA compliant security program.
- "Best Practice" is to build and maintain a security program based on a credible Framework.
- Security Risk Analysis is required – use a credible tool.
- There may be value (or even the emerging contractual requirement) for organizations to achieve an audited certification from a credible entity.

Thank you for joining us today!

QUESTIONS?

Appendix A
Resource Links

Resource	Link
HIPAA Security Rule Matrix	http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=f98695895303ff453f90dff84d86fe75&ty=HTML&h=L&mc=true&r=PART&n=pt45.1.164#ap45.1.164_1318.a
HHS-HIPAA for Professionals	http://www.hhs.gov/hipaa/for-professionals/index.html
NIST-Information Technology Portal	http://www.nist.gov/information-technology-portal.cfm
NIST-Managing Information Security Risk	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
NIST-Cybersecurity Framework (CSF) – Home Page	http://www.nist.gov/cyberframework/index.cfm
NIST-CSF Document (pdf)	http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
NIST-CSF and HIPAA Security Crosswalk	http://www.hhs.gov/sites/default/files/NIST%20CSF%20to%20HIPAA%20Security%20Rule%20Crosswalk%2002-22-2016%20Final.pdf
NIST-An Introductory Resource Guide for Implementing the HIPAA Security Rule	http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Resource	Link
NIST-HIPAA Security Rule Toolkit	http://scap.nist.gov/hipaa/
HealthIT.gov-Providers and Professionals	https://www.healthit.gov/providers-professionals
HealthIT.gov-Guide to Privacy and Security of Electronic Health Information	https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
HealthIT.gov-Information Security Policy Template	https://www.healthit.gov/node/289
HealthIT.gov-Mobile Device Privacy and Security Resources	https://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security
HealthIT.gov-Security Risk Assessment Tool	https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

Resource	Link
Google-Vendor Security Assessment Questionnaires	https://vsaq-demo.withgoogle.com/
HITRUST Alliance – CSF	https://hitrustalliance.net/hitrust-csf/
HITRUST Alliance – Healthcare Sector CSF Implementation Guide	https://hitrustalliance.net/documents/cybersecurity/HITRUST_Healthcare_Sector_Cybersecurity_Framework_Implementation_Guide.pdf
ISO-ISO/IEC 27001 - Information security management	http://www.iso.org/iso/home/standards/management-standards/iso27001.htm