MIPS/MACRA SECURITY RISK ANALYSIS

SRINI KOLATHUR
CISSP, CISA, CISM & MBA

Disclaimer

This webinar has been provided for educational and informational purposes only and is not intended and should not be construed to constitute legal advice. Please consult your attorneys in connection with any fact-specific situation under federal law and the applicable state or local laws that may impose additional obligations on you and your company.

WHO WE ARE …

EDUCATION
Online Training, Webinars and Customized Workshop

DIY TOOLKIT
Assessment Portal, Training, Forms and more …

CONSULTING
Professional services to help you with your Compliance needs

Srini Kolathur

CISSP, CISA, CISM, MBA

Director, EHR 2.0

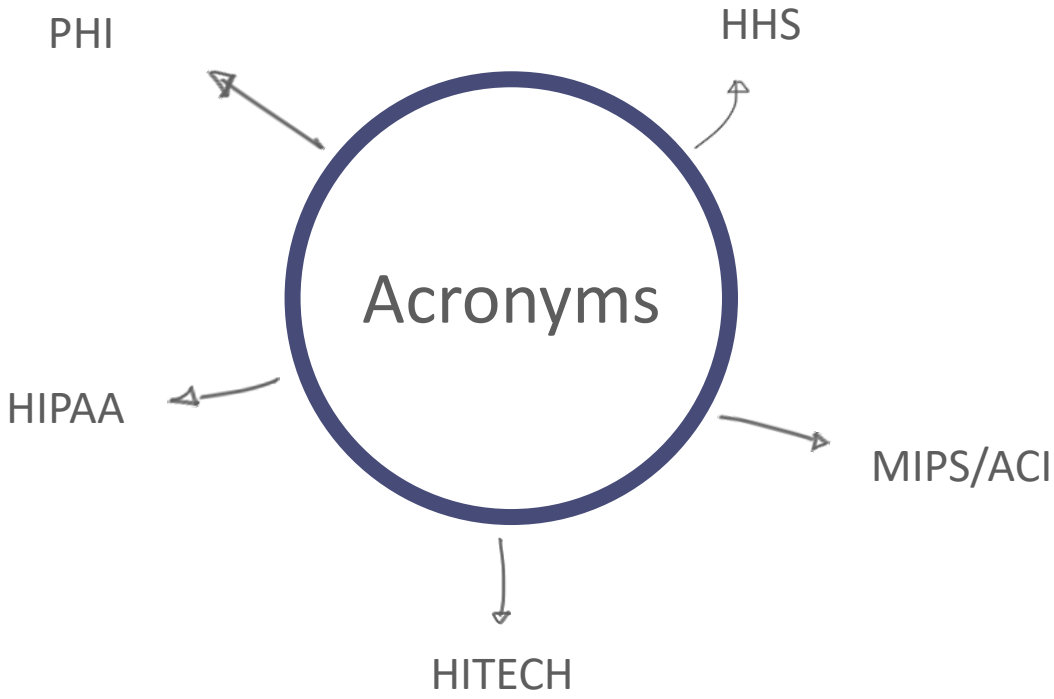
Srini's Background

- Security and Compliance
- Cisco IT Infrastructure
- HIPAA, PCI, Sarbanes-Oxley and ISO 27k Series
- A member of Rotary Club of Morrisville
- Interests: Running, healthy living and giving back

Agenda

- Attestation overview
- Best practices to handle security risk analysis
- Supporting documentation
- Meaningful Use/MIPS audit program overview
- Learning from audit findings
- Summary

TERMS YOU MAY HEAR …



MIPS – Advancing Care

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

In simple English: Need to have documentation on your patient data security practices/procedures.

Objective:	Protect Patient Health Information
Measure:	**Security Risk Analysis** Conduct or review a security risk analysis in accordance with the requirements in 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of data created or maintained by certified electronic health record technology (CEHRT) in accordance with requirements in 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the MIPS eligible clinician's risk management process.
Measure ID:	ACI_TRANS_PPHI_1

Definition of Terms

ONUS SCORE

s of base score measures to earn a
Care Information performance category.
opportunity to earn additional credit
bonus measure and/or activity.

Additional Information

- In 2018, MIPS eligible clinicians can report the Advancing Care Information Transition Measures if they have technology certified to the 2014 Edition, or technology certified to the 2015 Edition, or a combination of technologies certified to the 2014 and 2015 Editions.
- This measure contributes to the base score for the Advancing Care Information performance category. MIPS eligible clinicians must submit a "yes" for the security risk analysis measure to receive credit toward the base score. Submitting a "no" for this measure will result in a base score of 0%. More information about Advancing Care Information scoring is available on the QPP website.
- MIPS eligible clinicians must conduct or review a security risk analysis including addressing encryption/security of data created or maintained by CEHRT, and implement updates as necessary at least once each calendar year and attest to conducting the analysis or review.

MIPS SRA Scoring Criteria

- ✓ Base Score/Performance Score/Bonus Score
  - Required for Base Score: Yes
  - Percentage of Performance Score: N/A
  - Eligible for Bonus Score: No
- ✓ Must fulfill the requirements of base score measures to earn a base score in order to earn any score in the Advancing Care Information performance category. If the measure is not met, the entire score will be zero

Submitting a "no" for this measure will result in a base score of 0%

Security Risk Analysis Requirements Summary

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Scope: All eligible clinicians and hospitals
Program Type: Medicare/Medicaid
Requirement: Mandatory
Period: During the reporting year (1st Jan' to 31st Dec')
EHR Certification: 2014 and/or 2015 or combination

Attestation Overview

- Attestation is to legally state that you have demonstrated and met the objective
- Need to keep all supporting documentation (paper or electronic)
- Record keeping for six years
- Potential audit by CMS and State HHS (About 10%)

Frequently Asked Questions

- What is the difference between requirements of HIPAA/HITECH and MIPS Security analysis?
- When do we need to start and complete the MIPS SRA?
- Do we need to conduct comprehensive security risk analysis every year?
- How long does it take to complete the security risk analysis?
- What is the format of the final SRA report?

Scoping? It Depends …

- Organization Type
  - Small Practices, Hospitals, and Specialties
- Organization Size
  - Employees, Locations, Computer room vs. Data Center
- Complexity of Technology
  - Mobile, Network, Hosted, Cloud, etc.

Scoping is the most important part of Security Risk Analysis

Scope of MIPS Security Risk Analysis

Certified EHR system doesn't mean that your security risk analysis is done.

EHR System Safeguards

- EHR Security Best Practices
  - Configuration
  - Unique user accounts/IDs
  - Password requirements
  - Security patch updates
- Role-based Access to Patient Data
- Encryption of ePHI
- Audit logging

Cloud-based EHR requires additional safeguarding measures

Desktops/Laptops Safeguards

- Anti-virus, Malware and real-time protection
- OS and application patch updates
- Auto log-off (timeout) and Log-on password
- No unencrypted ePHI on desktop/laptop

Enforce policies via third-party agents or Active Directory

Mobile/Tablet Devices

- Password Protection
- Remote Wipe
- Texting and Encryption
- Centralized Mobile Device Management (MDM)
- BYOD Policy

Texting and e-mails are the common APPS used using mobile devices

Networking Devices

- Default Users/Pwd.
- Unnecessary services to be turned off
- Firmware update
- Log configuration/review
- Encryption of data-in-motion

Vulnerability scanning for on-premise EHR systems.

Removable Media

- Encryption
- Secure disposal
- Inventory of media

Other Systems

- E-mail
- HIE, Patient Portal, etc.
- Integration with 3rd party
- Copiers/Printers

https or VPN is the most secured way to access patient data

General and Administrative Areas

1. Security Program	Roles & Responsibilities External Parties
2. Security Policy	Policies and Procedures
3. Training & Awareness	Sanction, awareness training and reminders
4. Personnel Security	Background Checks, T&C, Termination Checklist
5. Physical Security	Secure Area
6. Operations Management	AV, Security Monitoring, Media Handling, Disposal, SOD
7. Incident Management	Process and Procedures
8. Business Continuity	Emergency access, Backup and DRs

Supporting Documentation

- Technical Security Risk Analysis Report
  - Dated
  - Scope must cover all ePHI data created/stored/transmitted by the EHR system
- Risk Management Plan
  - Prioritization of identified risks
  - Target date to mitigate the risks identified
- Policies and Procedures
- Review/Training Logs

Best Practices

1. Document

2. Develop risk management plan

3. Update the plan regularly

EHR 2.0 Compliance Services Portal

EHR 2.0 (Demo)

Security Risk Assessment

For Meaningful Use and HIPAA Compliance

HIPAA/HITECH Assessment

Includes Privacy, Security, and Breach Rules

Document Templates

Customizable Templates

Document	Date
Business Associate Contract Template	Jan. 7, 2016
Information Security Policy Template	Jan. 7, 2016
Policy on Breaches Template	Jan. 7, 2016

HIPAA Awareness Training

For Healthcare Workforce

Vulnerability Scan Reports

Includes IP, Web and Other Scan Results

Document	Date
IP Scan Example	April 13, 2016
Web Scan Example	April 15, 2016

Reports

Consulting reports prepared by EHR 2.0

Report	Date
Information Security Policy Example	April 14, 2016
ePHI Inventory List	April 14, 2016
Master Privacy Policy Example	April 14, 2016
Risk Management Plan and Checklist Example	April 14, 2016
Security Risk Analysis PDF	April 15, 2016
Security Risk Analysis	April 15, 2016

Data Breach Assessment Tool

Determine if a breach is to be reported

Employee Background Checks

Background Check Authorization Form

MU Audit Program - Overview

- Eligibility – Medicare/Medicaid Providers Applied for EHR Incentive
- Scope: MU Objectives and CQM
- Timeline: Up to 6 years
- CMS Medicare Audit Vendor: Figliozzi and Company
- Medicaid: State and Contractors
- Notification: Via Figliozzi and CMS Letter
- Audit: Pre-payment and Post-Payment

Audit Process

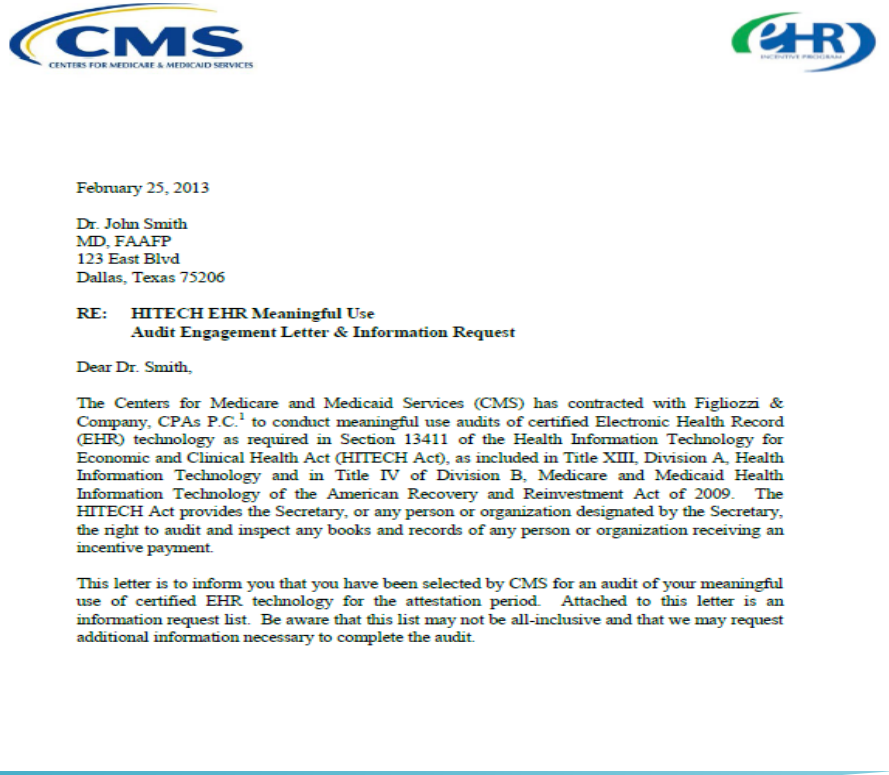
MU Audit Findings (Dec' 2015)

	Eligible Professionals	Eligible Hospitals
Audits	10,000	613
Didn't meet the requirement	22.7%	4.9%

- Security Risk Analysis – One of the major reasons for audit failure
- Most of the EPs and EHs who had to return the incentive amount did not have documentation of security risk analysis

Sample Audit Engagement Letter

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION



CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

EHR INCENTIVE PROGRAMS

February 25, 2013

Dr. John Smith
MD, FAAFP
123 East Blvd
Dallas, Texas 75206

RE: HITECH EHR Meaningful Use
Audit Engagement Letter & Information Request

Dear Dr. Smith,

The Centers for Medicare and Medicaid Services (CMS) has contracted with Figliozzi & Company, CPAs P.C.[1] to conduct meaningful use audits of certified Electronic Health Record (EHR) technology as required in Section 13411 of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), as included in Title XIII, Division A, Health Information Technology and in Title IV of Division B, Medicare and Medicaid Health Information Technology of the American Recovery and Reinvestment Act of 2009. The HITECH Act provides the Secretary, or any person or organization designated by the Secretary, the right to audit and inspect any books and records of any person or organization receiving an incentive payment.

This letter is to inform you that you have been selected by CMS for an audit of your meaningful use of certified EHR technology for the attestation period. Attached to this letter is an information request list. Be aware that this list may not be all-inclusive and that we may request additional information necessary to complete the audit.

Please supply all requested items by March 11, 2013, by utilizing one of the following methods:

1. Electronically uploading the information to our secure web portal (*see step by step instructions attached*)

2. Mailing the information to:

   Figliozzi & Company, CPAs P.C.
   585 Stewart Avenue
   Suite 416
   Garden City, NY 11530

The contracts between CMS and its contractors contain a confidentiality of information clause that state propriety information or data submitted by or pertaining to an organization cannot be released without the prior written consent of the organization. Additionally, the contractors are required to obtain written permission from CMS's contract officer whenever the contractor is uncertain on the proper handling of material under the contract. Further, if any information contained within the records your organization submits to CMS's contractors constitutes confidential information, as such terms are interpreted under the Freedom of Information Act (FOIA) (5 U.S.C. § 552) and applicable case law, CMS will protect such information from release when requested under FOIA in accordance with the Department of Health and Human Services regulations (45 C.F.R. § 5.65 (c)).

If you have any questions, please contact me by email at pfigliozzi@figliozzi.com or by telephone at (516) 745-6400 extension 302.

Sincerely,

Peter Figliozzi CPA, CFF, FCPA

Reference: CMS.GOV

Example: Document Request List - Eligible Professional

Centers for Medicare and Medicaid Services
Document Request List - Eligible Professionals

Medicare Electronic Health Record (EHR) Incentive Program

Please provide all of the documents requested below by the due date.
****Please separate your submissions by the item numbers listed below****

(A) Item Number	(B) Requested Documents
PART I - GENERAL INFORMATION	
1	As proof of use of a Certified Electronic Health Record Technology system, provide a copy of your licensing agreement with the vendor or invoices. Please ensure that the licensing agreements or invoices identify the **vendor, product name and product version number** of the Certified Electronic Health Record Technology system utilized during your attestation period. If the version number is not present on the invoice/contract, please supply a letter from your vendor attesting to the version number used during your attestation period.
2	Please provide a response to the following questions: a. At how many offices or other outpatient facilities do you see your patients? b. Please list each office or other outpatient facility where you see patients and indicate whether or not you utilize Certified Electronic Health Record Technology (CEHRT) in each office or other outpatient facility. **Office or Other Outpatient Facility** — **Utilize CEHRT? Yes / No** 1. 2. 3. c. If you utilize more than one office or other outpatient facility, could you please supply documentation which proves that 50% or more of your patient encounters during the EHR reporting period have been seen in offices or outpatient facilities where you utilize a CEHRT system? d. Do you maintain any patient medical records outside of your CEHRT system?
PART II - CORE SET OBJECTIVES / MEASURES	
3	For Core Measures #1 (CPOE for Medication Orders), 3 (Maintain Problem List), 4 (e-Prescribing), 5 (Active Medication List), 6 (Medication Allergy List), 7 (Record Demographics), 8 (Record Vital Signs), 9 (Record Smoking Status), 12 (Electronic Copy of Health Information), & 13 (Clinical Summaries), provide the supporting documentation (in either paper or electronic format) used in the completion of the Attestation Module responses (i.e. a report from your EHR system that ties to your attestation). Please Note: If you are providing a summary report from your EHR system as support for your numerators/ denominators, please ensure that we can identify that the report has actually been generated by your EHR (i.e. your EHR logo is displayed on the report, or step by step screenshots which demonstrate how the report is generated by your EHR are provided.)
4	Core Measure #15- Protect Electronic Health Information: Provide proof that a security risk analysis of the Certified EHR Technology was performed prior to the end of the reporting period (i.e. report which documents the procedures performed during the analysis and the results of the analysis). If deficiencies are identified in this analysis, please supply the implementation plan; this plan should include the completion dates.
PART III - MENU SET OBJECTIVES / MEASURES	
5	If attested to Menu Set Measures #2 (Clinical Lab Test Results), 4 (Patient Reminders), 5 (Patient Electronic Access), 6 (Patient-Specific Education Resources), 7 (Medication Reconciliation), or 8 (Transition of Care Summary), provide the supporting documentation (in either paper or electronic format) used in the completion of the Attestation Module responses (i.e. a report from your EHR system that ties to your attestation). Please Note: If you are providing a summary report from your EHR system as support for your numerators/ denominators, please ensure that we can identify that the report has actually been generated by your EHR (i.e. your EHR logo is displayed on the report, or step by step screenshots which demonstrate how the report is generated by your EHR are provided.) If attested to Y/N Menu Set Measures #3 (Patient Lists), 9 (Immunization Registries Data Submission), or 10 (Syndromic Surveillance Data Submission), please supply supporting documentation

Frequent Findings by Auditors

- Lack of formal security risk analysis report
- Reports are not comprehensive
- Not conducted during the reporting period

NEXT STEPS

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

1. 15-minute free consulting
2. DIY | Consulting | Managed Compliance
3. E-mail: info@ehr20.com

We provide audit support/guarantee for all our consulting and managed compliance customers

Additional Resources

- MU Audit Fact Sheet
- FAQ on MU
- Security Risk Analysis Tip Sheet by CMS
- Meaningful Use audit questions to Peter Figliozzi at (516) 745-6400 x302 or by email at pfigliozzi@figliozzi.com. Figliozzi and Company's website is http://www.figliozzi.com/

Upcoming Events

- OSHA for Healthcare Entities – 3/13
- Cybersecurity Framework (NIST) Assessment – 4/4

Visit ehr20.com/webinars to learn more

FIND US

CALL US
866-276 8309

SERVICE
info@ehr20.com

LOCATION
150 Cornerstone Drive ,
#202
Cary, NC

SOCIALIZE
Facebook
Twitter

Questions?

E-mail: info@ehr20.com

Call: 866-276-8309

EHR 2.0
SECURITY | COMPLIANCE | CERTIFICATION

Thank you!