Disclaimer

▲ This presentation was current at the time it was published or uploaded onto the web. Medicare and Medicaid policy changes frequently, so links to source documents have been provided for your reference.

▲ This presentation was prepared as a service to the public and is not intended to grant rights or impose obligations. This presentation may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage participants to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.
Agenda

1. Overview of M-CEITA
2. Security Risk Assessment Overview
3. HIPAA Audit Overview
4. Questions
Who is M-CEITA?

△ Michigan Center for Effective Information Technology Adoption (M-CEITA)

△ One of 62 ONC Regional Extension Centers (REC) providing education & technical assistance to primary care providers across the country

△ Founded as part of the HITECH Act to accelerate the adoption, implementation, and effective use of electronic health records (EHR), e.g. 90-days of MU

△ Funded by ARRA of 2009 (Stimulus Plan)

△ Purpose: support the Triple Aim by achieving 5 overall performance goals

**THE TRIPLE AIM**

3 Improve patient experience
Improve population health
Reduce costs

Meaningful Use
Certified Technology Infrastructure
Meaningful Use Support
Technical assistance, including workflow redesign, security risk assessment and MU compliance. (e.g. patient portal and clinical quality measures)

Security Risk Assessment
Support meeting the requirements of MU Measure: Protect Electronic Health Information, including an assessment using our exclusive tool.

Audit Preparation
A review of Meaningful Use attestation documentation using our exclusive Audit File Checklist, to correct any issues before completing the process.

Targeted Process Optimization (Lean)
A workflow analysis and redesign of core processes using Lean principles to increase efficiency and reduce duplication. (e.g. chart prep, doc. Management)

PQRS Support
Technical Assistance for the Physician Quality Reporting System including measure selection/optimization as well as reporting method selection and assistance.
Security Risk Assessment
Risk

People want to get value from the world

The world can be dangerous

People want to be secure from dangers

How do we get security in an insecure world?
Why Complete a Security Risk Assessment?

Consider three reasons to complete an SRA:

- Patient Safety
- Public Perception
- Compliance

All good reasons, but which is the top priority for your practice?
Patient Safety

“First, do no harm.”

▲ 112 million medical records were breached in 2015 alone
▲ Breached medical records can have real, serious consequences for victims:
  ▲ Average of over 12 million identities stolen every year
  ▲ Average cost: $5,130 per household
▲ Other concerns, such as privacy and stigma of health information
Public Perception

▲ Patients want access to their information and they want it to be safe
▲ **81% of patients** have concerns about privacy and security of EHR
▲ **60% of patients** believe that EHR use will result in more information being lost or stolen
▲ Patients, like any consumer, vote with their feet:
▲ **76% of consumers** report willingness to seek new providers after breach

**Other Considerations:**
▲ Increased probability of legal action against the covered entity by customers
▲ Customers less likely to share personal details with organization
Compliance

▲ Covered entities that suffer a breach and have **not performed a Security Risk Assessment**, or otherwise do not have an effective risk management program, face the **steepest penalties** from the Office for Civil Rights

▲ A lack of or incomplete SRA is the main reason providers **fail Meaningful Use** (MU) audits, resulting in loss of incentive money

▲ These costs are in addition to extra costs incurred by having **ineffective security** measures in place

  • Breach victims may pursue **legal action** for damages
  • Many healthcare providers have lost access to their data due to **ransomware** attacks or contract disputes
Risk is on the Rise

▲ Healthcare is the **leading US industry** for data breaches

▲ This is due to the relatively **high value** of medical records and relatively **low security** of their information systems (compared to, for example, banking and finance)

▲ ePHI breaches are increasingly attributed to hacking attacks, but **human behavior** is still a crucial factor (e.g. Anthem hack due to phishing attack)

▲ How can healthcare providers **protect their data** going forward?
  - Perform accurate and thorough risk **assessments**
  - **Manage** risk continuously
  - Increase use of **encryption**
  - **Train** all staff and providers on how to properly protect ePHI
  - Include medical and ancillary **devices** in risk assessments
SRA as a Meaningful Use requirement:

▲ Objective 1

– Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities

▲ Measure

– Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 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 its risk management process.
HHS Office for Civil Rights (OCR) Final Guidance

- **Scope** must include all ePHI in organization
- **Data collection** and methods must be documented
- Identify and document anticipated **threats** and **vulnerabilities**
- Assess **current security measures** in place
- Establish **likelihood** of threat occurrence
- Establish potential **impact** of threat occurrence
- Determine level of **risk**
- **Document complete** risk analysis
- **Periodic review** and **update**

*There is no “one way” to do an SRA, but every method must meet these objectives*
HIPAA Audit Program
HIPAA Security Rule

Security Rule
- Security Standards
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures
- Documentation Requirements
Meaningful Use Audits vs HIPAA Audits

▲ Meaningful Use Audits
- Random and based on prior audit results, if applicable
- Focus on timing and scope of SRA, documentation of key remediation activities (e.g. audit logs, compare risk results to corrective actions taken to address risks)

▲ HIPAA Audits
- Performed by the Department of Health and Human Services Office for Civil Rights (OCR)
- Examination of organization’s risk management program and security rule compliance
- Only a few hundred random audits per year
- CR investigations also occur following a breach
HIPAA Audit Pilot Program

▲ Mandated by the HITECH Act of 2009
▲ Provider compliance with Security, Privacy, and Breach Rules will be audited
▲ Most common Security deficiencies from 2012-2013 pilot audits:
  – Lack of or incomplete SRA
  – Unaware of Security Rule requirements
▲ OCR random audit program has begun in 2016
▲ Desk and Onsite Audits performed
▲ Covered Entities and Business Associates
▲ Program expected to be self-funding (unlikely to go away!)
OCR Audits Phase 2

Random Audits have begun in earnest

Key questions:

Who will be selected?
What initiates the audit?
What happens during the audit?
What happens after the audit?
Eligibility

▲ Any covered entity or business associate is eligible

▲ No exceptions!

▲ Phase 2 audits focused on pooling from a diverse array of entities

▲ Diverse based on: size, type, affiliations, public vs private, geography, and presence of existing OCR enforcement activity

- “OCR will not audit entities with an open complaint investigation or that are currently undergoing a compliance review.” - HIPAA Privacy, Security, and Breach Notification Audit Program website, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/ accessed 11/17/16
Contact Verification

▲ First step is verification of contact information

▲ On July 11, 2016, selected covered entities received emails to confirm the email address of the appropriate primary contact for that covered entity

▲ Failure to respond results in the same email address being used for future communication

▲ Make sure you check your junk mail or spam filters for “OCR”
Selection

▲ Pre-screening questionnaire
▲ Identification of Business Associates
▲ Random sampling of respondents will be audited

▲ Selected entities will receive a notification letter
  – Response expected within 10 business days

▲ Different entities under a single organizational umbrella may be chosen separately
Three Sets of Audits

1. Desk audits of Covered Entities

2. Desk audits of Business Associates
   - selection pool will be comprised largely of the BAs identified by the CEs in their document responses

3. Onsite Audits

▲ Audit program will be comprised of 200-250 audits in total
▲ Desk audits will focus on one of the three rules (Security, Privacy, or Breach Notification) for each auditee
▲ On-site audits will be comprehensive in scope
Desk Audits

▲ Entity must submit requested documents within ten (10) days of receiving notification letter

▲ OCR auditor will provide DRAFT findings based on submitted information

▲ Entity will have 10 business days to respond with comments

▲ If you do not cooperate during a desk audit, you could be selected for an onsite audit
Onsite Audits

▲ Notified via email
▲ Schedule entrance conference and information and expectations
▲ Conducted over three to five days onsite, depending on the size of the entity
▲ Will cover a wide range of requirements from the HIPAA Rules
▲ Entities will have 10 business days to review the draft findings and provide written comments
▲ Final audit report completed within 30 business days after response
▲ OCR will share a copy of the final report with the audited entity
▲ These are scheduled to begin in early 2017
Purpose

▲ Phase II designed to enable OCR to examine mechanisms for compliance

▲ Identify industry best practices

▲ Discover risks and vulnerabilities not surfaced through enforcement activities

▲ Enable us to get out in front of problems before they result in breaches
OCR’s Goals

▲ Audits are stated to be primarily a compliance improvement activity to help OCR to

- Better understand compliance efforts with particular aspects of the HIPAA Rules.
- Determine what types of technical assistance OCR should develop
- Develop tools and guidance to assist the industry in compliance self-evaluation and in preventing breaches
Document Request

▲ Auditees will receive request for documents via email
  – Two separate email requests
  – One will be for policies, procedures, and other related documentation
  – The other for a list of all the entity’s business associates

▲ Specify the documentation elements to be provided

▲ Business Associate listings must be submitted via email within 10 business days

▲ Email will provide link to secure online portal for submission of the rest of the documents
Expectations

Auditees are expected to:

▲ Submit **only** the policies and procedures that are relevant to the controls requested by the audit

  – If your information security policies are embedded within other policies or documentation (e.g. employee handbook), that information must be extracted and submitted on its own

▲ Provide clear, complete, and responsive documentation

▲ Submit documents on time (late submissions will not be considered)

▲ Include an explanation for why any requested documentation is lacking if that documentation is not available
Desk Audit Scope

▲ Privacy Rule Controls
   – **Notice of Privacy Practices & Content Requirements** §164.520(a)(1) & (b)(1)
   – **Provision of Notice - Electronic Notice** §164.520(c)(3)
   – **Right to Access** §164.524(a)(1), (b)(1), (b)(2), (c)(2), (c)(3), (c)(4), (d)(1), (d)(3)

▲ Breach Notification Rule Controls
   – **Timeliness of Notification** §164.404(b)
   – **Content of Notification** §164.404(c)(1)

▲ Security Rule Controls
   – **Security Management Process - Risk Analysis** §164.308(a)(1)(ii)(A)
What To Do During an Audit?

Be timely

Be cooperative

Be responsive

Be relevant

Bake cookies
What Happens After an Audit?

- Final audit report describes process, findings, and entity responses to draft findings
- Entity will be responsible for acting on audit findings, but a corrective action plan will not need to be submitted
- Enable OCR to better understand compliance efforts with HIPAA compliance
- Determine what types of technical assistance should be developed and what would be most helpful.
- Develop resources for entities based on information gathered from audits
- In-depth compliance reviews may be triggered by audit findings if significant threats to privacy and security are discovered
How Will Consumers Be Affected?

▲ Improve compliance with HIPAA protections
  – Uncover promising practices
  – Reveal why health information breaches are occurring

▲ OCR will create tools to help covered entities and business associates based on results of audit program
  – Technical assistance
  – Best practices

▲ Audit results expected to improve privacy and security practices by addressing concerns discovered
How Can You Prepare for an Audit?

▲ Make sure your HIPAA policies and procedures are complete, accurate, and organized
▲ If you haven’t completed a security risk assessment recently, you should do one
▲ Make sure your business associate agreements are in place and inventories
▲ Make sure your device / asset inventory is complete and up to date
▲ Address any issues identified in completed risk assessments
▲ Make sure all required security safeguards are in place
▲ Make sure all addressable safeguards are in place or have good risk assessment, explanation, and alternative measure are in place
▲ Document training of your workforce on HIPAA requirements and security best practices
Resources

Questions?

CONTACT INFO:

Andy Petrovich
734-302-4780
andy.petrovich@altarum.org