Meaningful Use Security and Privacy Measures: Audit Preparedness

11th Academic Medical Center Security & Privacy Conference

June 22, 2015

Dori Ledford, MHA, MBA
Meaningful Use Program Manager
Vidant Health

David Holtzman, JD, CIPP
VP Compliance
CynergisTek, Inc.
Agenda

• About Vidant Health and Corporate Quality’s Role
• About CynergisTek
• The Secret to Surviving MU Audits: Preparation
• Sharing Our Lessons Learned and Process for Audit Preparedness
• A Few MU Security Analysis Myths
• OIG Focus on Meaningful Use
• Q&A
About Vidant Health

- 29 counties (population 1.4M)
- ~12,000 employees
- 8 hospitals ~70 physician practices, home health, hospice, wellness centers and other health care services
- Affiliated with Brody School of Medicine at ECU
The Vidant Health Experience

• Quality owns Meaningful Use Designated workgroups, including:
  • Lead Roles and Project Managers, who plan and monitor all MU objectives
  • Permanent tools and resources to support ever-evolving MU requirements
  • Resources to manage and monitor Eligible Hospital (EH) and Eligible Provider (EP) specific progress and statuses
5 High Level Initiatives

1) Improve *quality*, safety, efficiency, and reduce health disparities

2) Engage patients and families

3) Improve care coordination

4) Improve population and public health

5) *Ensure adequate privacy and security protections for personal health information* (“Protect Electronic Health Information”)
About CynergisTek

**Founded in 2003**
CynergisTek has been providing services to our clients since mid-2003, but many of our clients have been with one or both of the founders since well before the company was founded.

**Synergistic**
The name “CynergisTek” came from the synergy realized by combining the expertise of the two co-founders – building scalable, mature information security programs and architecting enterprise technical solutions.

**Consulting Services**
CynergisTek provides consulting services and solutions around information security, privacy, IT architecture, and audit with specific focus on regulatory compliance in healthcare.

**Securing the Mission of Care**
CynergisTek Services are specifically geared to address the needs of the healthcare community including providers, payers, and their business associates who provide services into those entities.
MU Core Measure: Protect ePHI

Objective: Protect electronic health information created or maintained by the CEHRT through the implementation of appropriate technical capabilities.

42 C.F.R. § 495.6(f)(14)(i) and (l)(15)(i)
Security Risk Analysis Objective

• **Measures Stage 1:**
  - Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1); and
  
  - Implement security updates as necessary and correct identified security deficiencies as part of its risk
    - At least once prior to the end of the EHR reporting period and attest to that conduct or review. The testing could occur prior to the beginning of the EHR reporting period.

  - A security update is required if any security deficiencies were identified during the risk analysis.
Protect ePHI Measures Stage 2

**Measures Stage 2**

- Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1);

- Includes addressing the encryption/security of data stored in 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 the provider's risk management process.
The testing could occur prior to the beginning of the first EHR reporting period. However, a new review should occur for each subsequent reporting period.

Not required to report to CMS or the states on specific data encryption methods used.

EHs and CAHs affected by 42 CFR Part 2 should consult with the Substance Abuse and Mental Health Services Administration (SAMHSA) or state authorities.

In order to meet this objective and measure, an EH or CAH must use the capabilities and standards of CEHRT.
Certification & Standards Criteria

- Amendments
- Auditable events and tamper-resistance
- Audit report(s)
- End-user device encryption
- Authentication, access control, and authorization
- Automatic log-off
- Emergency access
- Integrity
- Optional– Accounting of Disclosures
# 1 Reason for MU Audit Failure

- It should not come as a surprise, since we are all here today for the 11th Academic Medical Center Security & Privacy Conference...

- **You May Already Know That...** The #1 reason organizations are unsuccessful with their Meaningful Use audits is failure to "conduct or review a security risk analysis“

- **Why?** This one Objective Measure impacts all other MU measures...Quite simply Meaningful Use requires sharing patient data in a **secured environment**-this translates across every measure regardless of stage

- **The Measure:** The Protect Electronic Health Information objective is included in the core set of both Stage 1 and Stage 2
Vital Lessons We Have Learned...

- Preparing for a potential audit is crucial in this ambiguous all-or-nothing program, where MU documentation shortfalls can lead to big losses.

- *It all comes down to preparation and documentation.*

- I have spoken to auditors and many believe that audits fail more often on lack of proof ... than on actual lack of compliance.

- **Step 1:** *Assume you will be audited* and plan each process with this in mind.

- **Step 2:** *Think like an auditor*
Vital Lessons We Have Learned Cont...

• If you haven’t been audited yet you haven’t had the privilege of seeing this ambiguous and sobering statement in your audit notification:

> “An audit may include a review of any of the documentation needed to support the information that was entered in the attestation. The level of the audit review may depend on a number of factors, and it is not possible to detail all supporting documents that may be requested as part of the audit.”

• This is when the gravity of the situation truly hits home if your organization has not yet proactively prepared for one. This is also when you learn just how vital advanced preparation is...
Meaningful Use in One Word: Ambiguous

- Meaningful Use Ambiguity is the cliché of political regulatory program language so why should audit request verbiage be any different?

- **Fight MU Ambiguity with:**
Step 1: Never Panic and Never Let Them See You Sweat (I swear the auditors can smell fear and I know for a fact they can sense a lack of confidence and planning—this part is more important than you think)

Fact: If you’ve been documenting and organizing the data, an audit wouldn’t be nearly as stressful because it’s simply a matter of producing the information. (stating the obvious...)

If you’ve been retaining the data but haven’t developed a system to easily access it, develop a plan to do that—NOW.

Keep in mind that Medicare can request information going back several years.
Vital Lessons We Have Learned Cont...

• **You are probably thinking:** “Well stating the obvious is great Dori, but what was Vidant’s *experience*?”

• We reacted as any good organization should: we created strategies from the process of being put through MU Audits by:

  • **Learning that we didn’t know quite what to expect until it hit**
    - We learned which documentation, operational and chain of communication areas needed ‘shoring up’

  • **Understanding the importance of the statement: “MU Takes a Village”**
    - We learned the importance of creating an MU Audit Committee that brought all the right people and departments to the table for support
Lessons from the Front Line

Remember when I said: **Step 1:** Never Panic and Never Let Them See You Sweat (...they can sense a lack of confidence and planning-*this part is more important than you think*)

**Tip:** Designate “point of contact” representative(s)

**This person must be:** confident, knowledgeable, have excellent communication skills and understand the vital difference between MU audits and all other types of clinical, legal or medical audits
A Representation of Our Audit Experiences

**Audit Program Process**

1. The Audit Process
2. The Letter
3. The Request for Documentation
4. Response and Request
5. Final Determination
6. Appeal Process
March 20, 2015

Report Number: [REDACTED]

NPI: [REDACTED] Sample: [REDACTED]

Dear [REDACTED],

This is to notify you that the Office of Inspector General (OIG) is conducting an audit of Medicare electronic health record (EHR) incentive payments made to eligible [REDACTED] nationwide. The objective of our audit is to determine whether Medicare expenditures for Medicare EHR incentive payments made to [REDACTED] were made in accordance with Federal requirements. The audit period includes all EHR incentive payments made from [REDACTED] to [REDACTED] during the audit period.

We have randomly selected the Medicare EHR incentive payment(s) made to NPI No. [REDACTED] during the audit period.

The OIG performs independent reviews of HHS programs and operations pursuant to the Inspector General Act of 1978, 5 U.S.C. App. § 4(a) (1). As a recipient of U.S. Department of Health & Human Services (HHS) grant funds, [REDACTED] is subject to OIG audits and other reviews. Pursuant to 45 CFR § 92.42(e), OIG has the right to timely and unrestricted access to all books, documents, papers, or other records that are pertinent to the Federal grant award.

Under the health information privacy regulation that implements the Health Insurance Portability and Accountability Act of 1996, providing the information requested by this letter is a permitted disclosure because it (1) is “required by law” to be produced to OIG as part of your participation...
...Lessons from the Front Line

• **Right People, Right Positions:** Assign an MU Audit Lead who has strong project management skills

• We involved team members that had the capability to *think like auditors*-this is why having MU reside with Corporate Quality was key

• **Involve:** Your Office of Audit and Compliance, Security Team, Legal, etc...

• **Get:** Get Organized, Get Confident, Get Moving!

• **Scope it Out:** Map out high-level overall process as it applies to your organizational structure
Get Granular: Create “audit trail” documentation with Visio diagrams, measure specifications and scorecards to assist with process mapping

- For each measure
- For each workflow
- Measure Specifications
- Screenshots
- Perform in-house mock-audits to QA each level of documentation
Lessons from the Front Line

Standardize, Standardize, Standardize…

• We standardized an enterprise MU audit process

• We communicated our organization’s audit expectations across all our EPs and hospitals

• We save all of the potential documentation we would likely submit for an audit in a single place

Examples:
- Create a Core Documentation Folder
- Create standardized MU Audit Checklists
- Create MU Audit Templates
- Create MU model folder formats
Lessons from the Front Line

And the most important lessons of all...

- **Never forget:** This will *all change* just as soon as you get a process down pat (...it wouldn’t be MU without this trait!)

- **Keep Up:** Stay on top of Regulatory Changes and make “MU Allies”

- **Fight MU Ambiguity with Clear Strategy:** all your actions must be filtered against a *clear strategy* and tempered appropriately or you risk making a difficult situation impossible

- **Constantly improve your processes:** especially those involving the Protection of electronic health information
A Few MU Security Analysis Myths...

Myth #1: Installing a certified EHR system fulfills the Security Risk Analysis Meaningful Use requirement.

- First of all, don’t believe it and yes, this is *False*.

- **Just the Facts**: Even with a certified EHR system implemented, you must perform a full Security Risk Analysis.

- **More importantly**: Security requirements address *all* electronic protected health information you maintain, not just what is in your EHR.
Myth #2: My EHR vendor took care of everything I need to do about HIPAA privacy and security.

• This is also False.

• Just the Facts: It is solely your responsibility to have a complete Risk Analysis conducted.

• Your EHR vendor can provide assistance, information and even training on the privacy and security aspects of their EHR product. However, EHR vendors are not responsible (nor desire to be liable) for making their products compliant with HIPAA Privacy and Security Rules.
Myth #3: Just completing a checklist will suffice for the Risk Analysis requirement.

- *Do not be tempted to take this shortcut. This is False.*

- **Just the Facts:** Checklists can be useful *tools*, especially when starting a risk analysis, but they fall short of performing a *complete* systematic Security Risk Analysis or documenting that one has been performed.

- *All* items for remediation noted on the checklist or in your Security Risk Analysis need to be completed to qualify for Meaningful Use.
Myth #4: I only need to do a Risk Analysis once.

- *This is False.*

- *Just the Facts: To comply with HIPAA, you must continue to review, correct or modify, and update security protections.*

- There is no mandatory timeline for updates, but a best practice is to do so at least once a year. Your annual Risk Assessment is valuable protection for patient information—and your business.
OIG Focus on Meaningful Use

- OIG FY 2015 Work Plan

  - Security of certified electronic health record technology

  - Perform audits of various covered entities receiving EHR incentive payments from CMS and their business associates, such as EHR cloud service providers, to determine whether they adequately protect electronic health information created or maintained by certified EHR technology

  - Engagements in each OIG region through the Office of Audit Services
Case Study in OIG Audit Process

• **Document Preparation**
  - 18 areas in which documentation requested prior to onsite engagement
  - Covers prior year attestation period and more recent information

• **Audit Team Onsite Visit – 2 weeks**
  - Exit interview with preliminary Notification of Findings
  - Opportunity for Remediation that can be reflected in final report
  - Interviews with staff involved in IT Security

• **Draft report** (about 3 months after onsite visit)
• **Covered entity comment/response to findings**
• **Final report is shared with CMS and OCR**
• **Rollup report summarizing all provider audits is posted to OIG Website**
OIG Audit Process

- Areas of Focus
  - Organizational Risk Analysis
  - Access Controls
  - Audit of alerts and logs from EHR
  - Patch Management
  - Encryption Security
  - System Scans
OIG System Scanning Tools

- OIG employs an appliance to perform database scanning for security safeguards
  - App Detective is optimized to scan
    - Oracle
    - Sybase
    - SQL Server
    - DB₂
    - Not effective on Cache
  - Reading for critical patches & updates
  - Effective access controls
Enforcement Outlook

• Takeaways from Joint OIG/DOJ Presentations:
  - OIG DC HQ Assoc. Counsel said OIGs approach to audit attestations has moved to a tool for incentive funds recovery
  - Asst. US Attorney from Dallas said its office is working with the OIG to investigate/prosecute Medicare fraud for knowing/false MU attestations
Questions?

David Holtzman
david.holtzman@cynergistek.com
512.405.8550 x7020

Dori Ledford
dori.ledford@vidanthealth.com
252.847.9697