OIG Security Audit: What You Need To Know

Executive Series Webinar
July 23rd, 2015
Today’s Speakers

Elana R. Zana
Attorney & Author
Ogden Murphy Wallace P.L.L.C.
ezana@omwlaw.com

Chuck Burbank
Director of Managed Privacy Services
FairWarning, Inc.
Chuck@FairWarning.com

Brian Stone
Manager, Customer Success
FairWarning, Inc.
Brian@FairWarning.com
Agenda

• OIG Work Plans
• Expectations - What OIG investigators will look for
• CMS vs OIG
• OIG audits related to Meaningful Use
• Audit readiness plan
• Audit controls
• Mapping to Audit protocols
OIG Audits

Elana Zana
ezana@omwlaw.com
206-442-1308
OIG Work Plans Target HIPAA & EHR

2014 Work Plan
• Security of Certified Electronic Health Record Technology under Meaningful Use

2015 Work Plan
• Security of Certified Electronic Health Record Technology under Meaningful Use
• Hospitals’ electronic health record system contingency plan
Multiple Government Entities Auditing HIPAA Security
OIG Security Audits
Security of Certified EHR Technology under Meaningful Use

“We will 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...

... Furthermore, business associates that transmit, process, and store EHRs for Medicare/Medicaid providers are playing a larger role in the protection of electronic health information. Therefore, audits of cloud service providers and other downstream service providers are necessary to assure compliance with regulatory requirements and contractual agreements.”
OIG Refuses Request For Information

• No information publicly available about:
  • Audit Process
  • How to prepare for an audit
  • Penalties related to audit results
  • Number of hospitals undergoing an audit
  • Audit reports
  • Benchmarks & best practices used as comparisons
Rumor Has It…

OIG Security Audit is not focused on individual entities, but is part of a comprehensive report that the OIG is developing based on its findings.
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. to conduct meaningful use audits of certified Electronic Health Record (EHR) technology as required in Section 15411 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.
EHR Incentive Program Audits: Double Jeopardy

Department of Health and Human Services
Office of Inspector General

Office of Audit Services, Region II
Jacob K. Javits Federal Building
26 Federal Plaza, Room 3900
New York, NY 10278

2014

Report Number:

Chief Executive Officer

Dear [Name],

The purpose of this letter is to notify you of our intention to audit the Electronic Health Record (EHR) System Information Technology Security Controls at Selected Hospitals Receiving EHR Incentive Payments. The objective of our audit is to assess if meaningful use requirements have protected the confidentiality, integrity, and availability of electronic protected health information (ePHI) in its EHR systems.
CMS vs. OIG

1. Meaningful Use Core Measure: Protect Electronic Health Information
2. To measure the objective, eligible hospitals must conduct security risk analysis of certified EHR technology per federal regulations
3. Figliozzi requests copy of Security Risk Analysis – does not analyze adequacy of Security Risk Analysis
4. Failure of CMS audit = Return of Meaningful Use $$$
CMS vs. OIG

1. OIG deeper dive into EHR security
2. Business Associates with access to EHR
3. Focus on EHR cloud service providers & EHR vendor
4. On-site Audit (2-3 weeks)
5. Interviews
6. Failure of OIG Audit = Fraud ??
OIG Audit Questionnaire

17 areas of interest including:

- EHR Risk Assessment, Audits & Reports
- EHR Security Plan
- Organizational Chart
- Network diagram
- EHR websites & Patient Portals
- Policies and Procedures
- System Inventory
- Tools used to perform vulnerability scans
- Central Log and Event Reports
- EHR System Users
- List of contractors supporting EHR & Network Perimeter Devices
Audit Question: Network Diagram

Provide the EHR network diagram (or network map) that shows your EHR network architecture including external connections.
Audit Question: Policies & Procedures

Provide copies of policies related to:

a. risk assessment
b. plan of action and milestones/corrective action plans
c. incident response
d. encryption
e. patch management
f. access controls
g. audit logging and/or audit controls
OIG Meaningful Use Audits
Medicare Meaningful Use Attestations

- Figliozzi Audits = 1 Year, only one Stage
- OIG Audits = Several Years, Possibly Stage 1 & Stage 2
- 30 days to respond
- Unknown if goal is individual audit or comprehensive report
Questions

• CEHRT documentation
• Information regarding EHR incentives received
• Questions Identical to CMS Audits:
  • Practice in multiple locations?
  • Core Set Measures
  • Menu Set Measures
  • Proof of Security Risk Analysis
• Questions follow Stage 1 2014 measures
AIU Audits

- Medicaid EHR Incentive Audit of hospitals…unknown if EPs
- 10 days to respond
- Must validate patient volume
- Deep dive into accounting related to calculating patient volume
- Must validate CEHRT
AIU Audits - Patient Volume

- Describe process for calculating Patient Volume
- In-depth information regarding patient volume - all patient data, not just Medicaid
  - *Please provide a detailed system-generated output report for your total patient volume for the 90-day reporting period used for the first-year payment attestation (and second-year payment attestation, if applicable). This report should include, at a minimum, the following criteria:
    - Provider Identifier
    - Service Date
    - Patient Name
    - Insurance Carrier/Insurance Plan
    - Charge Amount
    - Amount Paid

Why is this information needed for validating patient volume attestations?
AIU - Security

• In depth questions regarding hospital security, goes beyond meaningful use requirements.
  • Please answer the following questions concerning data security and integrity:
    a) Is a unique password required to access the EHR system?
    b) Did the hospital sign a confidentiality agreement with the EHR vendor?
    c) Does each user of the EHR system have their own unique electronic signature to sign off on documents and is the electronic signature time and date stamped?
    d) Can a document be edited/changed after it has been signed?
    e) Describe the hospital’s contingency plan if the EHR product goes offline? Please include in your description any use of backup files.
Audit Readiness Plan

1. Maintain documentation as required by the CMS EHR Incentive Program
   • 6 year requirement
   • Be able to pull this information upon request

2. Gather information consistent with OIG Audit Questionnaire

3. Evaluate health IT vendors and related Business Associate Agreement

4. Identify team that will respond to an OIG audit request

5. Conduct a mock audit to fully assess readiness
Elana Zana
(206) 442-1308
ezana@omwlaw.com
www.omwhealhlaw.com
@EZhealthlaw
It’s all about the evidence
• #1 deficiency in initial audits and #1 Technical Security Deficiency after the 115 audits
• Policy or procedure
• Evidence ongoing
• Criteria of the activities you monitor
• Evidence that criteria has been approved
## Example Audit Protocols – Audit Controls

<table>
<thead>
<tr>
<th>Section</th>
<th>Text</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>§164.312</td>
<td>§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
<td>Determine the Activities that Will be Tracked or Audited</td>
<td>Inquire of management as to whether audit controls have been implemented over information systems that contain or use ePHI. Obtain and review documentation relative to the specified criteria to determine whether audit controls have been implemented over information systems that contain or use ePHI.</td>
</tr>
<tr>
<td>§164.312</td>
<td>§164.312(b) Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
<td>Select the Tools that Will be Deployed for Auditing and System Activity Reviews</td>
<td>Inquire of management as to whether systems and applications have been evaluated to determine whether upgrades are necessary to implement audit capabilities. <strong>Obtain and review documentation of tools or applications that management has identified to capture the appropriate audit information.</strong></td>
</tr>
<tr>
<td>§164.312</td>
<td>§164.312(b) Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.</td>
<td>Develop Appropriate Standard Operating Procedures</td>
<td>Inquire of management as to whether procedures are in place on the systems and applications to be audited and how they will be audited. Obtain and review management’s procedures in place to determine the systems and applications to be audited and how they will be audited.</td>
</tr>
</tbody>
</table>
Evidence - Audit Controls (User Activity Monitoring)
## Example Audit Protocol – Incident Management

| §164.308 | §164.308(a)(6): Security Incident Procedures (§164.308(a)(6)(ii)) - Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. | Develop and Implement Procedures to Respond to and Report Security Incidents | Inquire of management as to whether there are formal or informal policies and/or procedures in place for identifying, responding to, reporting, and mitigating security incidents. Obtain and review the formal or informal policies and procedures and determine if incident response procedures are in place. Obtain and review the formal or informal policies and/or procedures and determine if incident response procedures are updated on a periodic basis based on changing organizational needs. Obtain and review formal or informal documentation to determine if the incident response procedures have been communicated to appropriate entity personnel. Obtain and review formal or informal documentation of procedures and evaluate the content relevant to the specified criteria in place for conducting post-incident analysis. Obtain and review formal or informal documentation to determine if post-incident analyses have been conducted. | Required |
Evidence - Incident Management
## Example Audit Protocol – Access Control

| §164.312 | §164.312(a)(2)(i): Access Control - Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions. | Ensure that All System Users Have Been Assigned a Unique Identifier | Inquire of management as to how users are assigned unique user IDs. Obtain and review policies and/or procedures and evaluate the content in relation to the specified criteria to determine how user IDs are to be established and assigned and evaluate the content in relation to the specified criteria. Obtain and review user access lists for each in-scope application to determine if users are assigned a unique ID and evaluate the content in relation to the specified criteria for attributing IDs. For selected days, obtain and review user access logs to determine if user activity is tracked and reviewed on a periodic basis and evaluate the content of the logs in relation to the specified criteria for access reviews. | Required |
### Alert & Investigation Dashboard

<table>
<thead>
<tr>
<th>Report Result - Untitled - (553 Records)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event Type</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>MR_REPORTS</td>
</tr>
<tr>
<td>VISIT_DIAGNOSES</td>
</tr>
<tr>
<td>CHARGES_VN</td>
</tr>
<tr>
<td>UOW_RELATED_Encounters</td>
</tr>
<tr>
<td>MR_REPORTS</td>
</tr>
<tr>
<td>VISIT_DIAGNOSES</td>
</tr>
<tr>
<td>CHARGES_VN</td>
</tr>
<tr>
<td>UOW_RELATED_Encounters</td>
</tr>
<tr>
<td>MR_REPORTS</td>
</tr>
<tr>
<td>VISIT_DIAGNOSES</td>
</tr>
<tr>
<td>CHARGES_VN</td>
</tr>
</tbody>
</table>

### Evidence – Access Control

The image displays a screenshot of the FairWarning platform, which is used for monitoring and analyzing access control activities. The interface includes various sections for dashboards, reports, enforced policies, alerts, investigations, and governance. The specific section shown is the Alert & Investigation Dashboard, which lists a series of events categorized under different types of access control activities. Each entry details the user name, date and time of the event, and the specific access control type.
Access Controls

• Processes for granting access to workforce & to third parties
• Processes for removing access
• Processes for updating access
• Elevated privilege management
• People with dual roles

What is your process for updating access when a worker changes jobs within the organization? Is it documented?
Ask the Experts

• Please submit via the WebEx Q&A or Chat windows to the right side of your screen.

For more information, please visit:

www.FairWarning.com
Thank you for attending!

Elana R. Zana
Attorney & Author
Ogden Murphy Wallace P.L.L.C.
ezana@omwlaw.com

Chuck Burbank
Director of Managed Privacy Services
FairWarning, Inc.
Chuck@FairWarning.com

Brian Stone
Manager, Customer Success
FairWarning, Inc.
Brian@FairWarning.com