Conducting a HIPAA Security Risk Analysis For MEANINGFUL USE, HIPAA Compliance and Good Business Practice

Presented for ICAHN by David A. Ginsberg
Agenda

- Deep Dive into the 15th Core Objective
- Conducting a risk analysis
- Remediation prior to attestation
- Self Assessment or Assisted?
- Round table discussion-problem solving for ICAHN members
Industry Recognizes

- Many CAHs and RHCs face a barrier when it comes to completing a HIPAA Security Risk Analysis based on:
  - Lack of understanding of this requirement under HIPAA
  - Lack of understanding of what is required for Meaningful Use
  - Lack of skills/resources and time to complete
## MU: Stage 1 Core Set Objectives

<table>
<thead>
<tr>
<th>Health Outcomes Policy Priority</th>
<th>Stage 1 Objective</th>
<th>Stage 1 Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Engage patients and families in their healthcare</td>
<td>Provide patients with an electronic copy of their health information (including diagnostic test results, problem list, medication lists, medication allergies, discharge summary, procedures), upon request</td>
<td>More than 50% of all unique patients of the EP, eligible hospital or CAH who request an electronic copy of their health information are provided it within 3 business days</td>
</tr>
<tr>
<td></td>
<td>Hospitals Only: Provide patients with an electronic copy of their discharge instructions at time of discharge, upon request</td>
<td>More than 50% of all patients who are discharged from an eligible hospital or CAH who request an electronic copy of their discharge instructions are provided it</td>
</tr>
<tr>
<td></td>
<td>EPs Only: Provide clinical summaries for each office visit</td>
<td>Clinical summaries provided to patients for more than 50% of all office visits within 3 business days</td>
</tr>
<tr>
<td>Improve care coordination</td>
<td>Capability to exchange key clinical information (ex: problem list, medication list, medication allergies, diagnostic test results), among providers of care and patient authorized entities electronically</td>
<td>Performed at least one test of the certified EHR technology’s capacity to electronically exchange key clinical information</td>
</tr>
<tr>
<td>Ensure adequate privacy and security protections for personal health information</td>
<td>Protect electronic health information created or maintained by certified EHR technology through the implementation of appropriate technical capabilities</td>
<td>Conduct or review a security risk analysis per 45 CFR 164.308(a)(1) and implement updates as necessary and correct identified security deficiencies as part of the EP’s, eligible hospital’s or CAH’s risk management process</td>
</tr>
</tbody>
</table>
Deep Dive into the 15th Core Objective

- Conduct or review a security risk analysis per 45 CFR 164.308(a)(1)

- What does the Security Rule say?

“Risk analysis (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”
Deep Dive

- This is a component of a broader regulatory standard known as risk management
- The concept of “CIA” is well established in the information security world
- In developing the HIPAA Security Rule, and specifically the risk analysis requirement, HHS relied upon guidance from organizations well versed in Information Security such as NIST
HIPAA Security Risk Analysis

- It is NOT a checklist!
- How do you “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI held by the covered entity?"
- There are steps that are defined by CMS, NIST and others
- These have been incorporated and made simple by PrivaPlan - both our do-it-yourself tools and service solutions
Details of a Risk Analysis

- It entails a formal review of risks to ePHI and your information security:
  - ePHI inventory and network or system characterization
  - Review of controls or safeguards
  - Review of threats and vulnerabilities including prior incidents
  - Criticality analysis
  - Review policies and procedures
  - Review likelihood of threat exploitation
  - Risk analysis
Details continued

- Your control analysis or review spans administrative, physical and technical areas and the other components in the HIPAA Security Rule
  - Workforce clearance
  - Access authorization
  - Termination procedures - don’t forget disabling web applications like eligibility portals!
  - Contingency planning and disaster recovery
  - Training
  - Sanctions
  - Incident reporting and response
Details continued

- Facility security
- Visitor access
- Emergency operations
- Maintenance
- Media and ePHI “life cycle”
- Paper disposal
- Business associate agreements
- Policies and Procedures
Details continued

- Review of prior incidents
- Review of technical controls
- Encryption controls
- Integrity controls (malware, use of secure portals)
- How to establish impact? First by defining ePHI criticality, then review threats and vulnerabilities
EHR Specific Focus

- Roles and permissions - security settings
- Audit logs
- Server location (even if you use a remote data center)
- Contingency and disaster recovery
- Periodic testing
- Specific MU areas like providing an electronic copy, patient summaries, patient reminders, patient access (portals), exchange of data
More on MU and the HIPAA SRA

The measure also states:

“...implement updates as necessary and correct identified security deficiencies...as part of the risk management process”

- What are updates? The results of a review of a prior HIPAA SRA, or an update to a SRA and/or updating the analysis
More on MU and the HIPAA SRA

- Correcting identified security deficiencies as part of a risk management plan:
  - Remember some of these may be Privacy/Security such as posting the Notice of Privacy Practices or using an up to date Business Associate agreement.
  - Of course, emphasis is on correcting those deficiencies that the use of an EHR exposes your organization to.
  - But it also refers to other security deficiencies that are gaps in compliance with the Security Rule.
More on MU

- What has to occur prior to attestation
- Certainly, conducting or reviewing a HIPAA SRA
- Identifying security deficiencies especially high risk-likelihood risks
- Correcting those deficiencies can be done as part of a risk management plan-based on your assessment of risk, and incorporating flexibility of approach
A follow up audit would expect a formal report to be on hand to prove you have done the risk analysis - and to show that you are remediating or managing gaps and deficiencies.

If you attest without doing the work, you will be risking fraud - being untruthful on your attestation documents and receiving federal funds.
Stage 2 Changes

- ONC and CMS mean business when it comes to safeguarding ePHI!!!!
- The preamble to Stage 2 Rule states:

“Due to the number of breaches reported to HHS involving lost or stolen devices, the HIT Policy Committee recommended specifically highlighting the importance of an entity's reviewing its encryption practices as part of its risk analysis.... Recent HHS analysis of reported breaches indicates that almost 40 percent of large breaches involve lost or stolen devices. Had these devices been encrypted, their data would have been secured.”
Stage 2 Changes continued

- The language for the HIPAA Core Objective measure stays the same but adds a key new concept:

Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest 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.
Stage 2 Changes continued

- The citations above reference the HIPAA Security Rule (the addressable encryption specification)
- The Certification Standards now expand the need to test if the Certified EHR can encrypt data on “end user devices” that remains after the session is “stopped” (or you have logged out of the application) - or whether the EHR prohibits data from remaining after the session
- Reviewing encryption of this kind of data at rest is a normal part of a good HIPAA Security risk analysis (as is evaluating data at rest on backup and storage media, servers and so forth) - but many organizations fail to review or act on this area!
Stage 2 Changes continued

- Encryption may not always be reasonable - but an alternative mechanism must be identified

The Preamble goes on to state:

“We propose this measure because the implementation of Certified EHR Technology has privacy and security implications under 45 CFR 164.308(a)(1). A review must be conducted for each EHR reporting period and any security updates and deficiencies that are identified should be included in the provider's risk management process and implemented or corrected as dictated by that process.”
ONC Guidance

- Providers can register for the EHR Incentive Programs anytime, but they can only attest after they have met the meaningful use requirements for an EHR reporting period. Only attest for an EHR incentive program, after you have fulfilled the security risk analysis requirement and have documented your efforts.

- Do not attest for an EHR Incentive program until you have conducted your security risk analysis (or reassessment) and corrected any deficiencies identified during the risk analysis. Document these changes.
When you attest to meaningful use, it is a legal statement that you have met specific standards, including that you protect electronic health information. Providers participating in the EHR Incentive Program can be audited.

If you attest prior to actually meeting the meaningful use security requirement, you could increase your business liability for federal law violations and making a false claim. From this perspective, consider implementing multiple security measures as feasible, prior to attesting. \textbf{The priority would be mitigating high-impact and high-likelihood risks}
The final HIPAA Omnibus Rule doesn't change the Security Risk Analysis requirement.

However, recent OCR enforcement has reiterated the necessity of conducting a Security Risk Analysis and fined organizations (including medical practices) for failing to do so!

Our analysis of the risk analyses that many practices have done as part of their MU attestation? Be prepared for audit deficiencies!!

OCR recognizes failure to conduct a RA or insufficient RA’s as a common compliance gap.
PrivaPlan Approach - Do it Yourself

- Demonstrated on the navigation guide next
Risk Analysis Toolset

PrivaGuides: What you need to know about the Security Rule.

1. Implementing the Security Rule
2. Choosing a Privacy & Security Official
3. A. Physical Security for Large Organizations
   B. Physical Security for Small Organizations
4. PHI Inventory
5. Risk Analysis (includes Risk, Threat, & Criticality Matrix)
HIPAA Security Risk Assessment

Next Step - Read the “Risk Analysis Tutorial”. This is a very important step that you must do before you “Start the Risk Analysis Walkthrough”
Document Templates: What You Need to Do for Your Risk Analysis

1. Start the Security Walkthrough
2. Risk Analysis Tracking Form
3. Business Associate Log
4. ePHI Use of Disclosure Summary
5. Job Responsibilities with Respect to PHI
6. Security Incident Form
7. Visitors Sign In Sheet
8. Workforce Log for Physical Security Access
Policies & Procedures

Things You Need to Implement in Your Organization as Standard Practices for all Employees

1. Procedures Manual
2. Security Policies Draft
3. Computer & Internet Use Policy
4. Laptops, Portables, & Devices Policy & Procedures
Training: Sharing the Importance of HIPAA Security with Your Staff

- Your Final Results must now be written down and documented on the "Risk Analysis Tracking Form" found under the Document Templates in order to complete your Risk Analysis.
<table>
<thead>
<tr>
<th>Risk</th>
<th>Date Found</th>
<th>Target Completion Date</th>
<th>Person or Team Assigned</th>
<th>Meaningful Use-MU</th>
<th>Meaningful Use Prior to Attestation-MU-A</th>
<th>Immediate Actions Necessary</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HIGH PRIORITY</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security incidents improperly handled.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This type of risk could be addressed by implementing response and reporting procedures for all security incidents. (This is a required implementation specification. See 164.308(a)(6)(ii).)</td>
</tr>
<tr>
<td>Computer crash causes permanent data loss.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This type of risk could be addressed by establishing a data backup plan. (This is a required implementation specification. See 164.308(a)(7)(ii)(A).)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This type of risk could also be addressed by establishing a data backup storage plan. (This is an addressable implementation specification. See 164.310(d)(2)(iv).)</td>
</tr>
<tr>
<td>Business cannot continue if the physical facility is not accessible. For example a flood or a fire in the building has made it impossible to get into your office.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This type of risk could be addressed by establishing a disaster recovery plan. (This is a required implementation specification. See 164.308(a)(7)(ii)(B).)</td>
</tr>
</tbody>
</table>
PHIsecure - a more robust tool
PHIsecure - a more robust tool
PHIsecure - a more robust tool
Consider these contributing factors in your decision making:

1. Have you ever had an outside review? If so, was it prior to implementation of EHR systems and was it more than 2 years ago?
2. Have you had significant IT infrastructure change?
3. Have you had any breaches or security incidents? Have any of these been “reportable”?
4. Do you have the internal resources?
Self Assessment or Outside Support

5. Do you need to justify or support enhanced security measures and controls?
6. Have you updated policies and procedures in the last two years?
7. Other threats and concerns?
Contact Information

Jon Langfitt – Computer Service Innovations
For Remediation Assistance
jlangfitt@csinov.com
585-319-7383

David Ginsberg
dginsberg@privaplan.com
1-877-218-7707