What is required of a compliant Risk Assessment?

ACR 2 Solutions President Jack Kolk discusses the nine elements that the Office of Civil Rights requires Covered Entities perform when conducting a HIPAA compliant Risk Assessment.
About ACR 2 Solutions

- ACR2 is a Georgia based developer of scalable real-time Risk Management and IT Compliance Software Solutions.
- Simple, easy to use Governance Risk Compliance (GRC) Information Security (IS) Compliance Solutions.
- Tools to support information security regulatory laws and regulations as follows: GLBA, HIPAA Privacy and Security, and PCI DSS.
- Risk and Compliance solutions for public, private, and government organizations.
- Former Technical Implementation Partner for GA-HITREC
- ACR2 is an HP Healthcare Alliance Partner
Introduction

- First of all, thank Medical Association of GA and for the opportunity to speak to all of you today.

- As a disclaimer, this is not legal advice, but it is documented and traceable advice. We pride ourselves in supplying you with the original source of our information.

- We live in a period of tremendous technological innovation that has massive implications to the healthcare industry,…the carrot being the Medicare/Medicaid EHR incentive program and the stick being ever stronger enforcement with HITECH increasing the civil penalties up to 30x’s the previous maximum fines!
Risk Assessments are the single greatest area where healthcare organization fail an audit according to the Office of Civil Rights (OCR).

Note in the 2012 pilot Audits 47 out of 59 (79%) providers had “No complete & accurate risk assessment.

Source: IAPP Conference March 7, 2013

Security Results

58 of 59 providers had at least one Security finding or observation

No complete & accurate risk assessment in two thirds of entities
- 47 of 59 providers,
- 20 out of 35 health plans and
- 2 out of 7 clearinghouses

Security addressable implementation specifications:
Almost every entity without a finding or observation met by fully implementing the addressable specification.
Increased Enforcement Promised

OCR attorney predicts spike in HIPAA fines

June 16, 2014 | By Susan D. Hall

The Office for Civil Rights' crackdown on HIPAA violations over the past year will "pale in comparison" to the next 12 months, a U.S. Department of Health and Human Services attorney recently told an American Bar Association conference.

Jerome B. Meites, OCR chief regional counsel for the Chicago area, said that the office wants to send a strong message through high-impact cases, according to Data Privacy Monitor.

The Office for Civil Rights has been levying fines to make healthcare entities take notice: nine settlements since June 1, 2013, have totaled more than $10 million. That includes a record $4.8 million fine announced in May against New York-Presbyterian Hospital and Columbia University.
Rumors about Risk Assessments: (that are dead wrong)

| The security risk analysis is optional for small providers. | **False.** All providers who are “covered entities” under HIPAA are required to perform a risk analysis. In addition, all providers who want to receive EHR incentive payments must conduct a risk analysis. |
| Simply installing a certified EHR fulfills the security risk analysis MU requirement. | **False.** Even with a certified EHR, you must perform a full security risk analysis. Security requirements address all electronic protected health information you maintain, not just what is in your EHR. |
| My EHR vendor took care of everything I need to do about privacy and security. | **False.** Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. It is solely your responsibility to have a complete risk analysis conducted. |
| A checklist will suffice for the risk analysis requirement. | **False.** Checklists can be useful tools, especially when starting a risk analysis, but they fall short of performing a systematic security risk analysis or documenting that one has been performed. |

Guide to Privacy and Security of Health Information
Version 1.2 060112
Where did we get our information?

- To this end the sources for this presentation are drawn from:
  - The OCR Final Guidance from OCR on what is required in a risk assessment
  - Supplemental guidance given by OCR employees in various interviews and documents

- Guidance on Risk Analysis Requirements under the HIPAA Security Rule
  - The Office for Civil Rights (OCR) is responsible for issuing annual guidance on the provisions in the HIPAA Security Rule.1 (45 C.F.R. §§ 164.302 – 318.)
  - HealthIT.gov and healthit.gov/sites/default/files/pdf/privacy/privacy-a...
  - ONC Guide to Privacy and Security of Health Information Version 1.2 060112
  - NIST Special Publications specifically NIST SP 800-30 and NIST SP 800-66 at NIST.gov/publication-portal.cfm
Risk Analysis

- OCR has stated that risk analysis is foundational, and must be understood in detail before meaningful guidance that specifically addresses safeguards and technologies that will best protect electronic health information.

- Although only federal agencies are required to follow guidelines set by NIST, the guidelines represent the industry standard for good business practices with respect to standards for securing e-PHI. Therefore, non-federal organizations may find their content valuable when developing and performing compliance activities.

- We begin the series with the risk analysis requirement in the Security Rule at § 164.308(a)(1)(ii)(A).
Why are we doing the Risk Analysis?

- All e-PHI created, received, maintained or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement “reasonable and appropriate” security measures to protect against “reasonably anticipated” threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process.

What is the difference between Risk Analysis and Risk Management in the Security Rule?

**Answer:** Risk analysis is the assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the electronic protected health information (e-PHI) held by a covered entity, and the likelihood of occurrence. The risk analysis may include taking inventory of all systems and applications that are used to access and house data, and classifying them by level of risk. A thorough and accurate risk analysis would consider all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage. Risk management is the actual implementation of security measures to sufficiently reduce an organization’s risk of losing or compromising its e-PHI and to meet the general security standards.
Why are we doing the Risk Analysis?

OCR:

- We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization. Instead, the Rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve.

- 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 [organization].
Are they really going to enforce this?

Former Director of OCR Leon Rodriguez at the HIMSS Privacy and Security Forum Boston Sept 23, 2013 “HIPAA is a valve, not a blockage,” stated HHS OCR Director Leon Rodriguez, at the OCR/NIST 6th Annual Conference on Safeguarding Health Information: Building Assurance through HIPAA Security.

"We hope to be off and running in the next calendar year," Rodriguez said at the HIMSS Privacy and Security Forum in Boston on Sept. 23.

Earlier, OCR had announced the audit program would resume sometime in fiscal 2014, which begins Oct. 1. OCR officials also indicated that business associates, as well as covered entities, will be audited in the permanent program because they’re liable for HIPAA compliance under the HIPAA Omnibus Rule.

In OCR's audits and breach investigations, "we will really look at the level of compliance at both covered entities and business associates," Rodriguez stressed in his Sept. 23 presentation.

Under the permanent program, audits will focus on vulnerabilities that might change year to year as new issues come into focus, Rodriguez said.

A major weakness found during the pilot audit program, as well as through OCR breach investigations, has been a lack of thorough risk analysis, he added.
Definitions:
Unlike “availability”, “confidentiality” and “integrity”, the following terms are not expressly defined in the Security Rule.

- **Vulnerability** - Vulnerability is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”

- Vulnerabilities, whether accidentally triggered or intentionally exploited, could potentially result in a security incident, such as inappropriate access to or disclosure of e-PHI. Vulnerabilities may be grouped into two general categories, technical and nontechnical.

- Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include: holes, flaws or weaknesses in the development of information systems; or incorrectly implemented and/or configured information systems.
Definitions:

- **Threat** - An adapted definition of threat, from NIST SP 800-30, is “[the potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”

There are several types of threats that may occur within an information system or operating environment.

Threats may be grouped into general categories such as natural, human (often insider and outsider), and environmental.

- Examples of common threats in each of these general categories include:
  - Natural threats such as floods, earthquakes, tornadoes, and landslides.
  - Human threats are enabled or caused by humans and may include intentional (e.g., network and computer based attacks, malicious software upload, and unauthorized access to e-PHI) or unintentional (e.g., inadvertent data entry or deletion and inaccurate data entry) actions.
  - Environmental threats such as power failures, pollution, chemicals, and liquid leakage.
Meaningful Use Stage 1, 2 and the draft of 3 require a annual Risk Assessment
But not just any risk assessment

<table>
<thead>
<tr>
<th>Protect Electronic Health Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objective</strong></td>
</tr>
<tr>
<td>Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.</td>
</tr>
<tr>
<td><strong>Measure</strong></td>
</tr>
<tr>
<td>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 management process.</td>
</tr>
<tr>
<td><strong>Exclusion</strong></td>
</tr>
<tr>
<td>No exclusion.</td>
</tr>
</tbody>
</table>

Eligible Professional Meaningful Use **Core Measures Measure 9 of 17**

**Stage 2**
Date updated: December, 2013

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. (added data at rest)
Definitions:

- **Risk** - An adapted definition of risk, from NIST SP 800-30, is: (see next slide for NIST definition)
  
  "The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . . [R]isks arise from legal liability or mission loss due to—
  
  1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
  2. Unintentional errors and omissions
  3. IT disruptions due to natural or man-made disasters
  4. Failure to exercise due care and diligence in the implementation and operation of the IT system."

- Risk can be understood as a function of 1) the likelihood of a given threat triggering or exploiting a particular vulnerability, and 2) the resulting impact on the organization.

- This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.
NIST Definition of Risk

“Risk is the net negative impact of the exercise of a vulnerability (by a threat source), considering both the probability and the impact of occurrence.” (NIST 800-30, page 1)
Risk Assessment Steps (NIST 800-30, page 8)

- Step 1 - System Characterization (Section 3.1)
- Step 2 - Threat Identification (Section 3.2)
- Step 3 - Vulnerability Identification (Section 3.3)
- Step 4 - Control Analysis (Section 3.4)
- Step 5 - Likelihood Determination (Section 3.5)
- Step 6 - Impact Analysis (Section 3.6)
- Step 7 - Risk Determination (Section 3.7)
- Step 8 - Control Recommendations (Section 3.8)
- Step 9 - Results Documentation (Section 3.9)
1. Scope of the Analysis - all ePHI that an organization creates, receives, maintains, or transmits must be included in the risk analysis. (45 C.F.R. § 164.306(a)).

- The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (also Business Ass’t’s, which may include your part time CFO, bookkeep and transcriptions) And contractors of BA’s.

- This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media. Electronic media includes a single workstation as well as complex networks connected between multiple locations. Thus, an organization’s

- risk analysis should take into account all of its e-PHI, regardless of the particular electronic medium in which it is created, received, maintained or transmitted or the source or location of its e-PHI.
2. Data Collection-The data on ePHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316 (b)(1).)

In compliance, as in health records, it must be documented.

- Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).)
- Organizations may identify different threats that are unique to the circumstances of their environment.
- Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI.

- This is becoming an area where automation is becoming a must, especially for larger practices.

- Although HIPAA doesn’t require penetration testing, using a scanner that assess the configuration is becoming unavoidable.

- Using SCAP allows security administrators to scan computers, software, and other devices based on a predetermined security baseline and determine if the configuration and software patches are implemented to the standard that they are being compared to.

- The national vulnerability database at http://nvd.nist.gov/ lists 63288 Vulnerabilities to computer systems! This makes it impossible to do by manually!

- Embedded devices. Fax machines copiers…
4. Assess Current Security Measures - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45C.F.R. §§164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

- This is not as straightforward as it may seem as many security controls are difficult to assess within the computer systems.

- As an aside, Windows XP is, with a few caveats, for most practices a major liability to you and your HIPAA compliance.

- At this point it should be obvious that if you can’t update and/or patch it, it is non compliant. This applies to all your machines that are connected to the network. We are aware that some organization have disconnected machines doing specific tasks to temporarily avoid compliance issues.
5. Determine the Likelihood of Threat Occurrence - The Security Rule requires organizations to take into account the likelihood of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

- The Security Rule requires organizations to take into account the probability of potential risks to ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are “reasonably anticipated.”

- The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of ePHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

- Again, this is becoming more and more difficult to do on your own…..
  - It’s certainly easier to do with a tool that has a risk calculation engine that has historical data.
6. Determine the Potential Impact of Threat Occurrence - The Rule also requires consideration of the “criticality” or impact, of potential risks to confidentiality, integrity, and availability of ePHI. (See 45 C.F.R. § 164.306(b)(2)(iv).)

- An organization must assess the magnitude (low medium or high) of the potential impact resulting from a threat triggering or exploiting a specific vulnerability.

- An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

- The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e- PHI within an organization.
7. Determine the Level of Risk - The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. (See 45 C.F.R. §§164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

- Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis.
- The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level.
- Software to implement this calculation is available from Symantec, Hewlett Packard and ACR 2 Solutions.
Sample ACR 2 Summary Report

Before and After

Risk Assessment Chart

Risk Assessment Number 10-08-09-1235025-000 - Report Generated October 12, 2009 - hipcompliancereporter.com

Risk Assessment Number 12-17-09-1261082383 - Report Generated May 10, 2010 - hipcompliancereporter.com

Risk Score

Risk Score
8. Finalize Documentation - The Security Rule requires the risk analysis to be documented but does not require a specific format. (See 45 C.F.R. § 164.316(b)(1).)

- The risk analysis documentation is a direct input to the risk management process (see next slide).

- We refer to the management process as the “cycle compliance”

- This should be ongoing. As the risk management needs to be implemented as determined by the risk management process.

- A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation.
STEP 8: CONTROL RECOMMENDATIONS

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization’s operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability.

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.
9. Periodic Review and Updates to the Risk Assessment - The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).)

- A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation.
- NIST requires updating risk assessments at least annually. OCR refers to NIST protocols as the “industry standard” for protecting ePHI.
Enforcement is on the Rise!

Extensive Outreach Efforts to Increase Awareness and Compliance

To effectuate the HITECH Act’s mandate to increase education to both HIPAA covered entities and consumers, and to address compliance deficiencies in the covered entity community identified by complaint investigations, compliance reviews, and the pilot audit program, OCR significantly amplified its public outreach and education campaign beginning in 2010 and continuing to today, with the goal of increasing compliance with the HIPAA Rules across the health care industry.
OCR HIPAA Complaints
Received and Closed

Total Investigated Resolutions
April 14, 2003 - December 31, 2012
- Corrective Action Obtained (Change Achieved) (66%) - 18,559
- No Violation (34%) - 8,007
Total Complaints Investigated 27,466

Status of All Complaints
April 14, 2003 - December 31, 2012
- Complaints Remaining Open (9%) - 6,931
- Complaints Resolved (91%) - 70,259
Total Complaints Received 77,190

* Referrals to DOJ - 509
For More Information

- Website – [www.ACR2solutions.com](http://www.ACR2solutions.com),

- Contacts
  - Debra Steen 404 625-2345
    - Debra.s@acr2solutions.com
  - Jack Kolk, 770 904-0997 or
    - jack.k@acr2solutions.com