HIPAA Privacy/Security Toolkits and the Meaningful Use Risk Assessment Requirement

A key issue for practices wishing to achieve meaningful use is the mandatory meaningful use item 15 requirement to “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.” (FR Vol. 75, No. 144 / 7/28/2010, p 44568). To help respond to this need, a number of public and private groups (1,2,3,4,5,6,7) have created HIPAA privacy and security “toolkits”. Public groups with toolkits include the American College Health Association (ACHA), the HHS Office of the National Coordinator (ONC) and the Healthcare Information and Management Systems Society (HIMSS).

All of the various toolkits have good program information and can be especially useful in setting up a risk management process. However, it appears that none of the toolkits claim at this time (March 2011) to meet the requirements of a 45 CFR 164.308 risk assessment as required by meaningful use item 15.

Meaningful Use Risk Assessment Requirements

The Office of Civil Rights (OCR) has the statutory responsibility to provide annual guidance on 45 CFR 164 compliance. The most recent OCR guidance document (8) from July 14, 2010, notes nine required elements for a 45 CFR 164.308 risk analysis.

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))
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).)
3. **Identify and Document Potential Threats and Vulnerabilities** - Organizations must identify and document reasonably anticipated threats to ePHI. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)
4. **Assess Current Security Measures** - Organizations should assess and document the security measures an entity uses to safeguard ePHI. (See 45 C.F.R. §§ 164.308(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)
5. **Determine the Likelihood 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).)
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).)
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).)
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).)
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).)
Software is available from a variety of sources to meet the item 15 risk assessment requirements (9, 10, 11, 12). The paper versions of NIST risk assessment documents are free to download at this time, although somewhat extensive (see photo at right).

Risk assessment programs that meet the requirements of 45 CFR 164.308 are dramatically different in purpose and capabilities from the HIPAA Toolkit programs. The table below compares the OCR 45 CFR 164.308 risk assessment requirements to the ACR 2 risk assessment program (9) and popular HIPAA Privacy and Security toolkits from ONC (2), HIMSS (1) and ACHA (3).

<table>
<thead>
<tr>
<th>OCR Risk Assessment Elements</th>
<th>ACR 2 HIPAA Rapid Risk Manager™</th>
<th>ONC toolkit</th>
<th>HIMSS toolkit</th>
<th>ACHA toolkit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Scope of the Analysis</td>
<td>NIST 800-66 compliant</td>
<td>page 4</td>
<td>Extensive resources on best practices and policies</td>
<td>less extensive than HIMSS</td>
</tr>
<tr>
<td>2. Data Collection</td>
<td>SCAP scan plus NIST 800-66 policy questions</td>
<td>page 5</td>
<td>Extensive resources on best practices and policies</td>
<td>less extensive than HIMSS</td>
</tr>
<tr>
<td>3. Identify and Document Potential Threats and Vulnerabilities</td>
<td>NIST 800-30/800-66 listing</td>
<td>page 7</td>
<td>Extensive resources on best practices and policies</td>
<td>less extensive than HIMSS</td>
</tr>
<tr>
<td>4. Assess Current Security Measures</td>
<td>NIST 800-66 compliant</td>
<td>pages 8-9</td>
<td>Extensive resources on best practices and policies</td>
<td>less extensive than HIMSS</td>
</tr>
<tr>
<td>5. Determine the Likelihood of Threat Occurrence</td>
<td>NIST 800-66 compliant</td>
<td>not included - refers to NIST 800-66 etc.</td>
<td>not included - refers to NIST 800-66 etc.</td>
<td>not included - refers to HIMSS</td>
</tr>
<tr>
<td>6. Determine the Potential Impact of Threat Occurrence</td>
<td>NIST 800-66 compliant</td>
<td>not included - refers to NIST 800-66 etc.</td>
<td>not included - refers to NIST 800-66 etc.</td>
<td>not included - refers to HIMSS</td>
</tr>
<tr>
<td>7. Determine the Level of Risk</td>
<td>NIST 800-66 compliant</td>
<td>not included - refers to NIST 800-66 etc.</td>
<td>not included - refers to NIST 800-66 etc.</td>
<td>not included - refers to HIMSS</td>
</tr>
<tr>
<td>8. Finalize Documentation</td>
<td>Full baseline report, online 45 CFR 164.308 compliance in detail.</td>
<td>implied</td>
<td>implied</td>
<td>implied</td>
</tr>
<tr>
<td>9. Periodic Review and Updates to the Risk Assessment</td>
<td>Online Gap Report auto-updated with each revision</td>
<td>Discussed page 1</td>
<td>Extensive resources on best practices and policies</td>
<td>less extensive than HIMSS</td>
</tr>
</tbody>
</table>

The ONC toolkit includes some good questions, but considers far fewer elements than the 105 involved in an NIST 800-66 assessment. The HIMSS toolkit has some excellent policies and practices elements, but the toolkit is not tightly organized. The ACHA toolkit is largely a subset of the HIMSS program.

At present, none of the toolkits include likelihood of occurrence, impact of occurrence or calculation of risk, elements that are key requirements of a 45 CFR 164.308 risk analysis as defined by OCR. While this omission is understandable – the calculations are fairly complex – they limit the ability of the toolkits to achieve item 15 meaningful use risk assessment compliance.
Attestation, Liability and Toolkit Disclaimers

Meaningful use attestation requires applicants for Medicare or Medicaid subsidies to state that they meet all the Stage 1 meaningful use criteria, including the creation of a 45 CFR 164.308 risk assessment. This is a significant legal step. In the EMR Registration Guide on page 14 the practitioner must agree that “I certify that the foregoing information is true, accurate and complete...the use of any false claims, statements or documents, or the concealment of a material fact...may be prosecuted under applicable Federal or State criminal laws...I agree to keep records...to demonstrate that I met all...Program requirements and to furnish those records...” False attestation is a federal crime, and the amount of money involved probably puts it into the felony range.

At least two groups are publicly declaring that the use of the ONC toolkit amounts to a risk assessment. The Practice Fusion EMR vendor states that use of the ONC toolkit “constitutes good-faith efforts to demonstrate a security risk review, and will stand as evidence supporting attestation of the Meaningful Use criteria.” (13). A March 23 email from the Georgia Regional Extension Center at Morehouse College scheduling a training session on the ONC toolkit calls the ONC toolkit a “risk assessment tool” although that phrase is not found in the document itself. No endorsement of the toolkit for risk assessment has yet been found on the ONC website.

The use of any toolkit to comply with legal requirements seems to contradict the disclaimer statements from the toolkit authors.

**ONC Toolkit - Disclaimer:** This guide was prepared to help small health care practices learn about the information security considerations that they may need to take into account as they become more reliant on health information technology. Use of this guide is voluntary and while it includes many important concepts, it alone will not enable, nor was it designed to ensure, that a health care practice complies with all applicable Federal and State laws.

**HIMSS – DISCLAIMER** - The Healthcare Information and Management Systems Society (HIMSS) Internet site on the World Wide Web, www.himss.org, is a service that is intended to provide useful information for HIMSS members, consumers and other interested persons. While it is the Healthcare Information and Management Systems Society's intent to always present accurate information, the Healthcare Information and Management Systems Society makes no warranties regarding the correctness of the information provided on this Internet site, www.himss.org, and HIMSS does not endorse, approve or certify such information, nor does it guarantee the accuracy, completeness, efficacy, timeliness, or correct sequencing of such information. HIMSS accepts no liability for damages of any kind resulting from reliance on any of the information provided therein. By proceeding to use this service, each user expressly waives any and all rights of action that he or she may have against the Healthcare Information and Management Systems Society arising out of use and/or reliance on the information on this service.

The Healthcare Information and Management Systems Society, and its officers, Trustees, employees and agents assume no responsibility for consequences resulting from the use of the information herein, or in any respect for the content of such information, including, but not limited to, errors or omissions, the accuracy or reasonableness of factual or scientific assumptions, studies or conclusions, ownership of copyright or other intellectual property rights, damages incurred if material infects or contaminates a user's system or information, and the violation of property, privacy or personal rights of others. No
guarantees or warranties of merchantability or fitness for a particular use or purpose are made by HIMSS with respect to such information.

At certain places on this HIMSS Internet site, live links to other Internet addresses can be accessed. HIMSS does not endorse, approve, certify or control these external Internet addresses and does not guarantee the accuracy, completeness, efficacy, timeliness or correct sequencing of information located at such addresses.

**American College Health Association (ACHA) - DISCLAIMER. PLEASE READ THIS FIRST.**

ACHA is pleased to provide the information on this Website. However, PLEASE READ THE TERMS CAREFULLY, because use of this site constitutes acceptance of these conditions. This information is NOT intended to provide legal or other professional services or advice. NO guarantee as to quality, timeliness, completeness, or applicability can be or is being made. In no event shall ACHA assume any responsibility or liability for this information or for any claims, damages or losses resulting from its use. ACHA makes no endorsement or representation whatsoever about any other Website that may be accessed through information on ACHA’s Website. ACHA does not endorse or accept responsibility for the content or use of such Website.

**Further Steps**

Given the severe liability involved with false attestation and the lack of clarity surrounding the use of HIPAA toolkits for risk assessment, ACR 2 Solutions and its commercialization partner, NWN, are seeking clarification directly from the Georgia REC, from ONC and from OCR. This whitepaper will be updated when such clarification is received.

**References**

**Suppliers of HIPAA Privacy and Security Toolkits**

1. HIMSS (Healthcare Information and Management Systems Society)  
2. ONC - HHS Office of the National Coordinator for Health IT  
3. American College Health Association  
4. Data Mountain  
5. Clearwater Compliance, LLC  
   [http://www.hipaasecurityassessment.com/signup](http://www.hipaasecurityassessment.com/signup)
6. HC Pro  
7. HITECH Security Advisors, LLC  

**Other references**

8. OCR guidance document on risk assessment  
9. [www.acr2solutions.com](http://www.acr2solutions.com)
10. [www.modulo.com](http://www.modulo.com)
11. [www.telos.com](http://www.telos.com)
13. Practice Fusion EMR  