Summary and Excerpts from ONC 2012 Meaningful Use Security Guidance

New ONC Guidance on Information Security

In May of 2011, ONC and the CMS Inspector General agreed after an audit of the ONC meaningful use security program that ONC needed to expand its security guidance beyond the bounds of the EMR. In May of 2012 that revised guidance became available (http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf). At 47 pages with copious referencing, the document can be overwhelming. This summary is an effort to excerpt the very useful and comprehensive ONC document into a more easily usable form.

One of the most important statements by ONC is on the cover and repeated elsewhere – *"The information contained in this guide is not intended to serve as legal advice nor should it substitute for legal counsel. The guide is not exhaustive, and readers are encouraged to seek additional detailed technical guidance to supplement the information contained herein."* This is absolutely true. However, as ONC also notes (p 17) that *"…outsourcing the security risk analysis function can make sense. RECs often provide this direct support. Another source of assistance may be your state or local medical association, or other professional medical association."*

An equally important insight is found on page 5. *"Good patient care means safe record-keeping practices. Do not forget that **an EHR** represents a unique and valuable human being: it **is not just a collection of data** that you are guarding – **it's a life**."* In 2010 a survey of California patients found that 68% were concerned about the privacy of their health information – up from 67'% in 2005 – see http://www.chcf.org/media/press-releases/2010/new-national-survey-finds-personal-health-records-motivate-consumers-to-improve-their-health#ixzz0ziYnva31 .

ONC notes, quite correctly, that the task of doing a meaningful use compliant risk assessment is not impossible for a practice. As noted on page 17 *"You however, can conduct the risk analysis yourself…You are still ultimately responsible for the security risk analysis even if you outsource this function."* It is not a trivial task. The standards set for a compliant risk assessment can use many procedures (p 11) but the guidance from the auditing agency, the Office for Civil Rights (link on p. 10) notes that *"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."* A partial set of the protocols needed for an NIST compliant meaningful use risk assessment is shown at right. They are free to download, but not very user friendly.

A lower cost alternative to developing or hiring an expert consultant is to use one of the commercial risk assessment products referenced on page 21 of the ONC guidance. Two of these products were on display at the Healthcare Information Management and Systems Society conference in February of 2012. Either is much more user-friendly than the various free tools (p 19, 46) or the NIST protocols shown at right. The Symantec product is sold through Allscripts (www.allscripts.com) . The Hewlett Packard Healthcare Alliance product is sold through ACR 2 Solutions (www.acr2solutions.com). Both are expert system computer model implementations of the NIST protocols shown at right, and prices for the ACR 2 Solutions product start at less than $1,000/year. See detailed information located at (https://www.acr2solutions.com/Documents/BasicRiskManagerDSr1.pdf) . The ONC page 21 guidance includes the excellent recommendation to *"Be sure to involve your EHR vendor, beginning with some basic questions."* Some EHR vendors (Allscripts, VersaSuite, Universal, XLemr, MedAZ, digiChart, others in negotiation) are providing referrals or discounted versions of these products, with enhanced coordination between the EMR and the assessment software.

Page 11 of the ONC report is an excellent summary of myths and facts. The page leads off with the statement that *"As with any new program or regulation, there may be misinformation making the rounds."* A few of the key facts include;

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.**

The notation that a checklist is insufficient to meet the meaningful use requirement is important, since it contradicts the advice from some (not all) RECs and EMR vendors that a checklist was adequate for attestation. Anecdotal evidence indicates that many, perhaps tens of thousands, of the 44,000 attesting provider from 2011 to March of 2012 used checklists to satisfy the item 15 requirements.

Attesting to meaningful use security without actually achieving meaningful use security can constitute fraud. As noted by ONC (p 27), "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."

Other Laws

Page 40 of the ONC guidance lists a number of laws other than HIPAA that affect the use of medical information. This is in addition to state laws, which can be significantly stronger than the federal version. California breach notification, for example, requires notification within five days, unlike the 60 day maximum under the federal statute.

Clarifications and Quibbles

While the ONC guidance document is unusually clear and well referenced, there are a very few items to take issue with, or at least discuss. For example, page 27 notes that *"Do not register and attest for an **EHR Incentive program**[40] until you have conducted your security risk analysis (or reassessment) and corrected any deficiencies identified during the risk analysis."* While this is absolutely true for Medicare, Medicaid has somewhat different rules. In the first year of subsidy, the Medicaid provider is only attesting that 30% of their patient encounters are with Medicaid patients. They do not attest to meaningful use until year 2 of the program. However, delaying the risk assessment until year 2 does leave the Medicaid provider out of compliance with HIPAA.

A second discussable statement is found on page 20, where ONC states that *"The risk analysis process is ongoing. There is no simple checklist that you can use to know that your security process is "done" or sufficient."* There is a partial exception from that rule for those risk assessments following the NIST protocols. On page 25 of NIST 800-30 (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf), a system for scoring risks on a 1-100 scale is described. Risks are characterized as "Low" with scores of 1-10, "Medium" with scores of 25-50 or "High" with scores from 50-100. On the same page it notes that "If an observation is described as low risk, the system's DAA must determine whether corrective actions are still required or decide to accept the risk. " A DAA is a "Designated Approving Authority" (800-30, p 2). So users with NIST 800-30 risk scores of 10 or less can justify observation only. Regular monitoring of risks however is still required and with a new risk assessment at least annually (ONC, p 20).