Meaningful Use Security Newsletter
July 30, 2012

CMS to Begin Audits of Attesting Providers

Law firm Ober Kaler has announced that CMS has begun audits of attesting providers under the HITECH Act. This has been confirmed by Bloomberg News. CMS has stated that it will audit 10% of attesting providers and that "…being found deficient on any one measure will cause provider to be out of compliance. In this case, CMS will recoup the provider's entire stimulus for the reporting period in question." And, according to at least one consultant, the first issue to be addressed in an audit will be the security risk assessment.

ONC Issues Dramatically Revised Security and Privacy Guidance

In May of 2011 the Inspector General of CMS audited the meaningful use security program at ONC and found it sorely lacking. The consent agreement between CMS and ONC calls for ONC to expand its security guidance from the EMR only to the entire information infrastructure. In May of 2012 the ONC issued dramatically revised security guidance that is apparently a result of this consent agreement. The 47 page guide and hundreds of pages of supporting documentation is somewhat hard to digest. A two page summary of the guidance is available here. There is a 90 minute webinar on the guidance available from HealthcareInfoSecurity.com.

Highlights of ONC Guidance

The ONC guidance is radically changed from previous recommendations. Page 11 of the guidance document is a summary of myths and facts. Key items include;

Myth	Fact
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 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.

EHR vendors are responsible for some of these myths. Many sales reps are claiming that their EHRs have all the capability needed for meaningful use. This is only true in a small number of cases. Allscripts, VersaSuite, Universal and XLEMR have NIST based risk assessment modules available. Hundreds of other certified EHRs do not. However, sales reps may claim capability they do not have. When confronted with the truth, one EMR sales rep commented that "I know it's a lie, but it helps sales. I am going to say it anyway". Buyer beware!

Another problem relates to checklists. Some vendors and some Regional Extension Centers (RECs) have in the past offered checklists as a solution to the risk assessment requirement. The new ONC guidance (page 11) disallows that approach.

Implications of New ONC Security Guidance

The new ONC guidance came out in May 2012, long after tens of thousands of providers had attested and received funding. Multiple conversations indicate that most providers either trusted their EMR vendor or used a checklist on advice from a vendor or an REC. This means that over 3,000 providers attesting in 2011 can be expected to fail their audits in 2012. A list of attesting providers as of March 31, 2012 is available here.

Attesting Provider Options

The 36,000 attesting vendors subject to audit have few options. They can hope to not get caught, although at 10% the odds of a CMS audit are much higher than for an IRS audit. Pencil and paper item 15 risk assessment services are expensive but available. A list of the NIST protocols involved in a meaningful use risk assessment is shown at right. They are free to download but require significant expertise to use.

Software for creating an NIST based meaningful use risk assessment is available from multiple vendors. Software is useful for practices down to one provider. Beginning Friday August 3 ACR 2 Solutions is offering a 90 day, 25% discount on risk assessment software to anyone on the 2011 attesters list. An order form is found here.

This discount offer is open to three classes of customer.

1. Attesting providers on the list.
2. Regional Extension Centers buying either directly or through attesting providers.
3. Certified EMR vendors.

Longer term reseller agreements are available. Contact project manager Robert Peterson for details.

Opt-out of Newsletter

To stop receiving this newsletter, click on the link.