Guest Author Steve Spearman: A Meaningful Use Audit, What to Expect: A Doctor Speaks

If you read my alert from August or the followup article on Audit Red Flags to Avoid, you are aware that CMS hired an accounting firm, Figliozzi & Company, to audit the compliance of eligible providers and eligible hospitals that had already received payment under the meaningful use (MU) program. According to a report from the GAO as many as 20% of eligible providers and 10% of eligible hospitals may be audited, on a post-payment basis to confirm that they actually met the requirements of the program.

I recently had the opportunity to interview a physician that is currently going through the audit process with Figliozzi & Company (an edited transcript of the interview can be found here). Although he wishes to remain anonymous, he was willing to report on his experience and provide redacted copies of the correspondence and requests that he has received from the auditors.

This physician, whom I will call Dr. Jones, is a primary practice physician in the Southwestern United States. His initial stage one reporting period was in 2011 and he attested in 2011. He implemented a certified EHR application, SoapWare, in 2008 so he was already an experienced EHR user when meaningful use rolled around. According to a report published by the CDC, only about 17% of physicians in 2008 had implemented an EHR with most of the functionality that would be required by certified EHR's under meaningful use. So when HITECH and meaningful use became law in 2009, it is not surprising that Dr. Jones would be among the first round of physicians to attest. As you may know, the initial reporting period for stage one was a 90 day period that had to occur

during a calendar year. This 90 day period is the period in which you have to collect and use your EHR and exceed the thresholds established for meaningful use. And for those measures requiring a Yes/No attestation, you have to affirm that you met the measure.

First I want to lay out the facts and then do some analysis.

In the third quarter of 2012, Dr. Jones received an email from Figliozzi & Co. informing him that his "facility has been selected by CMS for a HITECH meaningful use audit."[i] All the correspondence with Figliozzi has been via email, something that surprised Dr. Jones and me. The email contained a number of attachments which you can view here, here, here and here.

None of the original documents specified the period for which Dr. Jones was being audited. Figliozzi might have assumed it that it was obvious because Dr. Jones had only attested and received payment once, for his initial 90 day attestation in 2011. However, that reporting period was long out of Dr. Jones mind and, as it was nearing the end of 2012 and the end of his first full year reporting period, he assumed that the audit was related to his current reporting period, the full 2012 calendar year. In his own words, "…it wasn't very clear. Because at the same time that we received this (the audit letter) we were getting ready to attest for 2012." Clearly, this betrays a common knowledge deficit about the meaningful use audit program. The post-payment audit program is only for those that have already attested and received funding. The email from Figliozzi could have been clearer on that point.

Dr. Jones prepared some data for 2012 and sent it along to Figliozzi and Company, and hoped that he was done.

He was not.

A few weeks later, Dr. Jones received a terse email from a

different auditor within the company. An attachment to the email clarified that the audit was for the 2011 reporting period and requested additional information. Specifically, Dr. Jones needed to provide additional supporting evidence such as :

1. Proof of possession. In other words, Dr. Jones needed to provide evidence that he owned the software at the time of attestation and that it was of a certified version of the software. The types of documentation might include invoices, contracts, or licensing agreements but the documentation needed to specify dates and versions in order to be acceptable.
2. Provide documentation specifically related to the Core Yes/No measures:
    1. Core # 2 – Drug Interaction checks – provide evidence that the capability was running during the entire reporting period or demonstrate that the capability cannot be disabled.
    2. Core # 11 – Clinical Decision Support (CDS) – provide a schedule of alerts from the period or demonstrate that the capability cannot be disabled
    3. Core # 14 – Exchange of Clinical Information – Screenshots from the EHR demonstrating a test exchange of clinical data or an email confirming receipt of the exchanged data.
    4. Core # 15 – Protect Electronic Health Information – a risk analysis report dated prior to the end of the reporting period.
    5. In addition, Dr. Jones needed to provide proof that he had had met the two Yes/No Menu measures that he had selected:
        1. Menu # 3 – Patient Lists – A list of patients with a specific medical condition generated by the EHR.
        2. Menu # 10 – Syndromic Surveillance Data Submission – Screenshots from the period

> which document a submission of test syndromic surveillance data or a dated email/letter from an agency indicating receipt of such data.

Dr. Jones scrambled to put together the supporting documents and mailed them to Figilozzi and Co. within the required deadline. He is waiting to hear from them.

Here are a few thoughts about Dr. Jones experience and the things to consider prior to attesting.

In order to be eligible for funding, an eligible provider must meet all the core measures and five (out of ten) menu measures. Most of the measures are reported directly out of the EHR but a few are not. These tend to be the measures that present the most problems with documenting compliance. They have the common characteristic that they are Yes/No measures and the affirmation needed cannot be auto-generated from data in the EHR. Based on a specific EHR, you might be able to document compliance using reports or the audit system of the EHR. For example, many EHR's should be able to document and retain the creation of alerts for Core # 11, the CDS measure. This should also be true of Core # 2, the drug interaction check measure and Menu # 3, the Patient List measure.[ii]

Core # 14, Exchange Clinical Information and Menu # 10, should be readily provable if you successfully sent data to the receiving parties and received an email or letter affirming receipt. However, the standards explicitly allows that the test does not have to be successful. If it is not successful, it is crucial that providers take screenshots of the entire process of the tests as they are conducting them. Interestingly, both of the measures have exclusions, one of which likely applied to Dr. Jones situation. If you claim an exclusion on any measure, be sure to thoroughly document the reason for the exclusion with supporting evidence.

That leaves Core Requirement # 15 which is of course, a focus of Health Security Solutions practice. So here are some thoughts on meeting this requirement:

- As we have reported before, the standard states that the risk analysis must be conducted during the reporting period (or prior to the initial 90 day reporting period).
- Organizations do NOT have to outsource this requirement but it will make sense for many organizations to do so. Typical physician practices have neither the expertise nor the resources to conduct a risk analysis.
- The audit specifies that they would expect to see a "report" documenting that a risk analysis was completed.
- The exact process for conducting and reporting a risk analysis is not defined in the regulations. So what will be acceptable to an auditor? Your best bet is one that complies with NIST Guidelines, specifically Special Publication 800-30. Appendix K of that document provides an outline of what should be included in a report. Page 29 lists the specific broad tasks associated with risk analysis[iii]:

One last thought. For many practices, the MU requirements seems overwhelming. This is especially true of the risk analysis requirement. Smaller practices are not flush with cash and even more bereft of resources. This is one reason we developed and introduced our Risk Analysis in a Box Lite service line, designed specifically for small providers. Please call us if we can be of service to you.

In future post, I hope to provide more reflections, ideas and advice on the MU audit program by seeking guidance from credible experts and others invested in seeing it, and its benefactors, succeed. I will also keep readers updated on the status of Dr. Jones.

Steve

Steve Spearman, Founder and Chief Security Officer for Health Security Solutions, has been in the healthcare industry since 1991. After spending more than a decade observing health care providers struggle with the HIPAA Security and Privacy regulations, he founded Health Security Solutions in the summer of 2010 to help organizations minimize and mitigate the financial, legal, and compliance risks associated with running health care organizations.

Steve alongside his team of security experts, have helped healthcare providers qualify for millions of dollars worth of stimulus funding through a wide range of HIPAA consulting services and solutions, including his very own risk assessment method, Risk Analysis in A Box.

To learn more about Steve, Health Security Solutions, and the services they provide please visit www.healthsecuritysolutions.com.

---

[i] I wonder if the use of the word "facility" implies that all physicians at a single practice would be audited at the same time. Dr. Jones is a solo practitioner so we can't know from his example.

[ii] I intend to contact an expert in the field related to the capabilities and certification requirements of certified EHR's and will report on that in a later alert.

[iii] Risk Analysis Tasks according to NIST 800-30.

- Identify threat sources that are relevant to organizations
- Identify threat events that could be produced by those sources;
- Identify vulnerabilities within organizations that could

be exploited by threat sources through specific threat events and the predisposing conditions that could affect successful exploitation;

- Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful;
- Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources (through specific threat events); and
- Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with the risk determinations.