Prepare Now for Meaningful Use Attestation and Compliance Audits

By Diana Warner, MS, RHIA, CHPS, FAHIMA

A warning issued in 2013 by the Centers for Medicare and Medicaid Services (CMS) has come to pass. "Meaningful use" Electronic Health Record (EHR) Incentive Program audits have begun. The College of Healthcare Information Management Executives (CHIME) reported that out of their 1,400 member organizations, almost 100 received audit notices in October 2013, totaling six percent of membership. In order to protect incentive payments earned through the meaningful use program, organizations need to be prepared for every audit contingency and know exactly what to expect. Organizations also need to avoid common mistakes that could lead to an audit and follow best practices for staying compliant to meaningful use standards.

How Audits Work

CMS has contracted with only one vendor, Figliozzi and Company, to conduct meaningful use audits, which can be performed on any type of organization that attested to the meaningful use program and received an incentive payout. When selected for an audit, an initial request letter from the auditor will be sent electronically from a CMS e-mail address and will include the audit contractor's contact information. The e-mail address provided during registration for the EHR Incentive Programs will be used for the initial request letter.

The initial review process will be conducted at the audit contractor's location, using the information received as a result of the initial request letter. Additional information might be needed during or after this initial review process, and in some cases an onsite review at the provider's location could follow. Organizations have about three weeks to submit all of the requested documentation for the audit.

CMS Using Pass or Fail Audits

Organizations must verify that the reporting from their certified EHRs has synchronized data from multiple systems, validate that the reported clinical quality measures (CQMs) have calculated correctly, and ensure compliance with standard terminologies has led to accurate reporting across their systems.

Organizations that fail to pass the audit of even one meaningful use measure will be required to return their entire incentive payment. Organizations have 30 days to return the money. There is no interest or claims adjustment, and the check is to be made for the same amount that was received.

Information Governance Supports Incentive Strategy

Organizations must be able to ensure that data are consistently and accurately captured within the EHR in order to ensure that all measures reported to CMS through the meaningful use program are accurate. Organizations need to monitor all the necessary sources of data for meaningful use compliance to ensure that the data sources are reliable and organized, as well as identify which fields in the EHR system(s) must be completed for meaningful use data collection. Organizations should have a program that verifies output from their EHR(s) and looks at synchronizing data from multiple systems, validating CQMs, and ensuring compliance with standard terminologies.

Achieving the many stages of the EHR Incentive Programs requires that the provider C-suite, clinicians, and health IT professionals are on the same page to ensure that the right systems, training, and fail-safes are in place when eligible providers

are going through their reporting periods. In addition, a provider must prove that the required functionality was activated during the meaningful use reporting period.

Document Meeting Core and Quality Measures

All attested measures need to be supported by documentation in the event of an audit. Attesters should review the meaningful use specification sheets and frequently asked questions (FAQs) reports published by CMS. The specification sheets and FAQs resolve many ambiguities created by the measures themselves, and the auditors rely upon them as interpretive guidance to the measures. Organizations will want to identify and confirm that members responsible for the meaningful use program understand all the measures, reports, and validation of the information related to the attestation.

Physical documentation is required for proof of attestation. Documentation may include dated screen captures that demonstrate meeting the measure during the reporting period, security risk assessment reports, or an e-mail from an immunization registry confirming receipt. The primary documentation that will be requested in all reviews is the source document(s) that the provider used when completing the attestation. This document should provide a summary of the data that supports the information entered during attestation. Ideally, this would be a report from the certified EHR system, but other documentation may be used if a report is not available or the information entered differs from the report.

Documentation required for audits, at minimum, will include:

- The numerators and denominators for the measures
- The time period the report covers
- Evidence to support that it was generated for that eligible professional, eligible hospital, or critical access hospital (i.e., identified by National Provider Identifier (NPI), CMS Certification Number (CCN), provider/practice name, etc.)

Common Meaningful Use Mistakes

Below are common meaningful use attestation mistakes that could cost organizations during an audit.

- **Not documenting the meaningful use strategy.** The attesting organization should document the reasoning behind those core measures that were excluded and menu measures that were not chosen.
- **Not identifying responsibility.** A committee, not just one person, should be assigned to take responsibility for the audit process and requests for documentation.
- **Not retaining sufficient documentation.** Keep all documents and reports used to attest for meaningful use. Do not assume that the reports can be recreated.
- **Ignoring requirements.** If an organization is not clear what a requirement means, seek clarification. Do not just attest “yes” to yes/no meaningful use criteria.
- **Blaming the EHR vendor.** The vendor does not have the sole responsibility for ensuring the measures chosen by the facility are met.
- **Not performing or updating the security risk assessment.** HIPAA and meaningful use require periodic risk asessment updates.

Security Risk Assessments, EHR Certification Targeted

A security risk analysis of certified EHR technology must be conducted or reviewed and updates implemented as necessary at least once prior to the end of the EHR reporting period. Providers must then attest that the analysis took place. A new review must occur for each subsequent reporting period. Meaningful use auditors are demanding proof that risk assessments have been conducted during the meaningful use attestation period in question, rather than before the periods begin. These risk assessments must also show that any deficiencies found were completely remediated before the reporting period ended.

EHR adopters must prove that their systems are certified for meaningful use during the entire reporting period. This process also includes verifying that version numbers and upgrades are up-to-date and correct for the particular stage of meaningful use. Proof is required for every version during the meaningful use reporting period.

Although the summary document is the primary review step, there could be additional and more detailed reviews of any of the measures, including a review of medical records and patient records. An audited organization should be able to provide documentation to support each measure to which it attested, including any exclusions claimed by the provider. Organizations should expect three to four rounds of requests for information from the auditors. The auditors are demanding screen shots showing various aspects of compliance. Submitting ancillary proof of compliance, such as a checked-off list of tasks performed, is insufficient.

References

CMS. "42 CFR Parts 412, 413, 422, and 495: Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule." *Federal Register* 75, no. 144, July 28, 2010. http://www.gpo.gov/fdsys/pkg/FR-2010-07-28/pdf/2010-17207.pdf.

CMS. "Frequently Asked Questions." July 1, 2013. http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/FAQ.html.

Mace, Scott. "Latest Wave of MU Audits Delivers a Fresh Scare." *HealthLeaders Media*. October 29, 2013. http://www.healthleadersmedia.com/content/TEC-297810/Latest-Wave-of-MU-Audits-Delivers-a-Fresh-Scare##.

Murphy, Kyle. "Best practices for meaningful use pre- and post-audits." *EHR Intelligence*. July 15, 2013. http://ehrintelligence.com/2013/07/15/best-practices-for-meaningful-use-pre-and-post-audits/.

Tate, Jim. "What not to do in a meaningful use audit." *Healthcare IT News*. October 21, 2013. www.healthcareitnews.com/news/what-not-do-meaningful-use-audit.

Diana Warner (diana.warner@ahima.org) is a director of HIM practice excellence at AHIMA.

Article citation:
Warner, Diana. "Prepare Now for Meaningful Use Attestation and Compliance Audits" *Journal of AHIMA* 85, no.3 (March 2014): 52-53.