Health Care Providers Should Expect Meaningful Use Audits

In the past five years the Medicare and Medicaid Electronic Health Record Incentive Programs have disbursed billions in financial support to providers that adopt and demonstrate a meaningful use of certified electronic health record (EHR) technology. Given this level of funding, it is little wonder that the Centers for Medicare and Medicaid Services (CMS), which administers the programs, is required by law to audit Medicare-participating providers that accept these federal dollars. (Medicaid providers are typically audited under a separate process handled by the state's Medicaid agency or its contractor.)

While eligible providers (EPs), which include certain health care professionals and hospitals, may be selected for audit due to an irregularity in attested data, the majority will simply be selected at random. Therefore every EP should plan on the inevitability of a meaningful use audit and take steps to prepare.

The Audit Starting Point

The audit clock starts upon receipt of a letter from Figliozzi and Company, the current CMS contractor for pre- and post-payment audits. The communication is sent to a provider's email on record, so an EP should ensure the email address provided is in working order and is regularly monitored.

The audit letter requests documentation to support the attestation data for meaningful use objectives, clinical quality measures, and payment calculations. The requested information must be submitted within 14 days and generally falls within three categories:

- Proof of a meaningful use certified EHR
- Quality measure, core, and menu objective data documentation
- Proof of a security risk assessment with corrective action plan

The review is conducted as a desk audit using the information provided to the request letter. It is important to note that statements without supporting documentation would not be considered responsive to a document request. An auditor may also conduct an onsite review and request a demonstration of the certified EHR system that was used to attest.

Document, Document, Document

In light of the two-week window for an audit response, it is imperative that providers ensure compliance with meaningful use measures on an ongoing basis.

Use of A Certified EHR

To qualify for an incentive payment EPs must successfully adopt certified EHR technology and use it to achieve specific objectives. But it is important to note than only EHRs certified for the EHR incentive programs satisfy the requirement—an EHR certified for other CMS programs may not necessarily meet this objective. If in doubt, check the list of certified EHR products available on the U.S. Department of Health and Human Service's Office of the National Coordinator's website.

CHRISTIAN & BARTON, LLP
ATTORNEYS AT LAW

For additional information:

Jonathan M. Joseph
jjoseph@cblaw.com
804.697.4125

Maintain current documentation from the selected EHR vendor that identifies the EHR system and version in use. Be aware that some vendors may have older versions of EHRs that are not certified. Accordingly, any system upgrades should be examined closely as changes may affect certification status.

Documentation Should Be Secure, Accessible and Organized

CMS deems the provider responsible to maintain all documentation that supports meaningful use and quality measures data for at least six years from attestation submittal. This documentation should be securely stored and readily accessible to IT and compliance staff.

In particular, it is vital to have easy access to a copy of the primary report generated by the EHR system. That report should, at a minimum, document the numerators and denominators for all percentage-based measures, the time period that the report covers, and evidence to support the report was generated for the specific provider. Such evidence can include the provider's National Provider Identifier, CMS Certification Number, or provider name. Ideally, each page of the report should include such identification.

The following information should also be stored as it may be requested in an audit:

- Proof of ownership of a certified EHR
- Core and menu measure MU Reports used to enter attestation data
- Documentation for "Yes" attestation measures to evidence such measures have been met
- Report of the clinical quality measures that are reported by the EHR
- A copy of the attestation that was submitted and all supporting documentation used while preparing for attestation
- Documentation of exclusions of measures
- Transmission certifications (such as dated screenshots from the EHR system that document a test exchange of key clinical information with another provider during the reporting period)

Where applicable, this information may be maintained in the form of screenshots taken from the EHR during the reporting period. Screenshots should show the date; provider name; name and vendor of the EHR; and the EHR version number. In addition, patient-specific information should be redacted before providing the report to the auditors, unless the auditor requests otherwise.

Pay Attention to Security Risk Assessments

Meaningful use measures require providers conduct or review security risk assessments as required by the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Risk assessments must specifically address new technologies that are adopted, such as an EHR system, as well as any changes made to such technologies. Neglecting the risk assessment is the leading reason for failed audits, and missteps in this area not only place a provider at risk of losing incentive payments, but can also result in further investigations or sanctions by the Department of Health and Human Services' Office for Civil Rights for being HIPAA non-compliance.

Adverse Findings and Appeals

An EP deemed ineligible for an incentive payment by an audit must pay back any incentive already received unless the auditors' decision is overturned on appeal. Intentional fraudulent activity will be reported to the FBI and/or the Department of Justice for further investigation and potential sanctions. In addition, a false attestation could be the basis for liability under the Federal False Claims Act or similar state laws.

A provider may appeal audit results to CMS. To begin this process, providers must complete and file an Appeal Filing Request (available on CMS' website) within 30 days of the adverse audit determination letter. Appeals are only processed if all documentation outlined in the Request is provided at the time of submission.

Limit Stress with a Plan

While an audit is stressful, this stress can be minimized with careful preparation and attention to detail. Key steps include assigning responsibility for email monitoring, and investing and maintaining a storage system that facilitates quick access to EHR documentation. Retaining knowledgeable counsel can also help providers navigate the audit and appeal processes.