Bloomberg BNA

BNA's
Health Law Reporter™

Meaningful Use Program Audits: What to Expect and Recommended Practices

BY AMMON R. FILLMORE AND STEPHANE P. FABUS

The measures and objectives that an eligible provider must satisfy to receive an incentive payment continue to dominate public discourse regarding the ''meaningful use'' program. This intense focus on the incentive payments is understandable given that the Centers for Medicare & Medicaid Services (CMS) estimates that eligible providers will receive more than $27 billion in meaningful use incentive program payments over the course of the meaningful use program.[1] However, as eligible providers receive and exhaust available incentive payments, the meaningful use program fundamentally shifts from an incentive program to a compliance program. Forward-thinking eligible providers will anticipate this shift and plan ahead for the continuing role the meaningful use program will play in health care operations, notably the ongoing occurrence of meaningful use program audits . Failure to prepare for, comply with and pass an audit can not only result in an eligible provider being required to return incentive payments that were already distributed, but may also result in Medicare reimbursement adjustments and other legal actions and investigation.

Overview of the Audit Program

Just as the HITECH Act authorized the meaningful use program incentive payments, the related final rules published by the Department of Health and Human Services on July 28, 2010, and Sept. 4, 2012, provide additional details and requirements regarding the audits.[2] All eligible providers attesting to the meaningful use program may be audited. According to Robert Anthony, deputy director of the HIT Initiatives Group at CMS, approximately one in 20 eligible providers can anticipate an audit.[3] CMS contractor, Figliozzi and Co., performs audits on eligible providers enrolled in the Medicare meaningful use program as well as those dually eligible providers participating in both the Medicare and Medicaid meaningful use programs.[4] Because eligible pro-

[1] *EHR Incentives & Certification: What is Meaningful Use?*, HealthIT.gov, http://www.healthit.gov/providers-professionals/ehr-incentives-certification.

Ammon R. Fillmore is an associate with the Indianapolis office of Hall, Render, Killian, Heath & Lyman PC. His practice focuses on advising hospitals, health system and physician organizations on corporate and health law related matters including regulatory and compliance, contracting and information systems.

Stephane P. Fabus is an associate with the Milwaukee office of Hall, Render, Killian, Heath & Lyman PC. Fabus focuses her practice on assisting health care clients in a wide range of areas, including general business transactions and services and regulatory and compliance matters.

[2] Medicare and Medicaid Programs; Electronic Health Record Incentive Program, 75 Fed. Reg. 44314 (July 28, 2010) (to be codified at 42 C.F.R. pts. 412, 413, 422, and 495); Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed Reg. 53968 (Sept. 4, 2012) (to be codified at 42 C.F.R. pts. 412, 413 and 495). *Also* 42 C.F.R. § 495.316, which requires states to submit a state Medicaid HIT plan that includes a detailed plan for monitoring, verifying and periodic auditing of the requirements for receiving incentive payments. However, under 42 C.F.R. § 495.312, a state may allow CMS to conduct the audits and handle any subsequent appeal of whether eligible hospitals are meaningful EHR users on the state's behalf.

[3] Joseph Conn, *Feds aim to audit 5% of participants in EHR program*, Modern Healthcare (April 22, 2013), http://www.modernhealthcare.com/article/20130422/NEWS/304229954.

[4] *EHR Incentive Programs Audits Overview*, CMS (February 2013), https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_Audit_Overview_FactSheet.pdf.

 ISSN 1064-2137

viders participating in only the Medicaid meaningful use program can expect their applicable state contractor to conduct an audit, this article focuses primarily on the Medicare audits.

Eligible providers can expect either a prepayment audit or a post-payment audit.[5] If an eligible provider is selected for a prepayment audit, CMS will not release the incentive payment until the eligible provider presents supporting documentation to validate the submitted attestation. Conversely, eligible providers selected for post-payment audits are required to submit the necessary supporting documents to validate the attestation after CMS has already made an applicable payment. Eligible providers selected to be audited will receive notice by a letter sent electronically to the email address provided during the eligible provider registration process. Eligible providers should take the necessary steps to ensure the email address provided during the registration process is regularly maintained to avoid missing important communications and forgoing valuable time to respond to the audit.

Preparing for a Meaningful Use Program Audit

Audit preparation begins upon enrollment in the meaningful use program and requires the provider to have an actionable compliance plan to prevent and navigate an audit, to mitigate any possible damages and to minimize disruptions to health care operations. Any meaningful use compliance program should, at a minimum, include a compliance team and procedures to successfully document the meaningful use program attestation.

Develop a Meaningful Use Compliance Team

The success of the meaningful use program and the use of certified electronic health record technology (CEHRT) is not dependent solely upon the information technology department. The meaningful use program affects individuals from across multiple departments, including legal, medical records, compliance, information technology, administrative, finance, human resources and, perhaps most importantly, the clinical and medical staff. A well-designed meaningful use compliance program will include a meaningful use compliance team composed of individuals from across these and perhaps other departments, each with assigned and documented roles and responsibilities. Ensuring that each person on the meaningful use compliance team has distinct and assigned responsibilities is crucial to avoiding missteps and, when necessary, facilitating a root cause analysis.

In addition to a meaningful use compliance team, eligible providers should focus on developing a strong relationship with the CEHRT vendor. A successful meaningful use compliance program can benefit from the CEHRT vendor's unique position as the CEHRT developer. The CEHRT vendor also can be an indispensable resource in developing actionable processes and workflow to document a successful attestation.

Document Meaningful Use Compliance

The foundation of a successful meaningful use compliance program is consistent, routine and structured documentation. Whether an eligible provider successfully navigates an audit often depends upon an organization's culture and practices, in particular, proper document retention. An audit will require documentation, both written and electronic, of an eligible provider's attestation for a meaningful use program incentive payment for each applicable reporting period. Eligible providers should confirm that there is documentation to support: 1) attestation data for all meaningful use program objectives and clinical quality measures for a minimum of six years after an attestation; and 2) payment calculations, such as cost report data, that follow applicable documentation retention processes.[6]

Eligible providers should be conscious that documentation may differ depending on the requirements of each particular meaningful use measure. For example, CMS suggests that to demonstrate compliance for the Stage 1 measure for generating lists of patients by specific conditions, the eligible provider may utilize a report from the CEHRT dated during the reporting period. However, for the Stage 1 measure requiring electronic exchange of clinical information, CMS suggests that eligible providers maintain dated screenshots from the CEHRT that document a test exchange and a letter or email from the receiving provider confirming a successful exchange with applicable details.[7]

Not all CEHRT have the same functionalities for maintaining audit logs. This means that eligible providers should be conscious of whether documenting a successful meaningful use program will require regular screenshots and printed reports to confirm attestation. Likewise, eligible providers with multiple CEHRT should confirm that documentation is captured and maintained across all applicable practice areas. A successful meaningful use compliance program will identify what documentation should be maintained for each meaningful use measure and whether the documentation is electronic or in paper format. Documentation should also include any communications with your CEHRT vendor, the Office of the National Coordinator (ONC) and publications such as the ''frequently asked questions'' or tip sheets published by CMS.

Penalties for Audit Failure

A failed audit can disrupt eligible providers' health care operations, require repayment and reimbursement adjustments and raise questions regarding compliance. If an eligible provider fails an audit, CMS does allow an appeal; however, absent a successful appeal, CMS expects the eligible provider to refund the meaningful use program incentive payment for the applicable reporting period. A failed audit also means that an eligible provider did not successfully attest under the meaningful use program. Beginning in October 2014 for eligible hospitals and in 2015 for eligible professionals and criti-

[5] *Id.*

[6] *Id.*

[7] *EHR Incentive Programs Supporting Documentation For Audits*, CMS (February 2013), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHR_SupportingDocumentation_Audits.pdf. *Also*, *Stage 2 EHR Incentive Programs Supporting Documentation For Audits*, CMS (February 2014), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage2_AuditGuidance.pdf.

  HLR ISSN 1064-2137

cal access hospitals, failure to successfully attest to the meaningful use program can result in a payment adjustment to an eligible provider's reimbursement. The following is a summary of the payment adjustments the eligible provider may face under the meaningful use program and other penalties that could be imposed under the False Claims Act and the Health Insurance Portability and Accountability Act (HIPAA).

Adjustments for Eligible Hospitals

Eligible hospitals participating in either the Medicare or Medicaid meaningful use incentive programs will soon be subject to Medicare payment adjustments for a failed attestation.[8] Eligible hospitals that are not meaningful CEHRT users, and therefore failed to successfully attest, will be subject to a payment adjustment beginning on October 1, 2014. This payment adjustment applies to the percentage increase to the Inpatient Prospective Payment System (IPPS) payment rate such that these hospitals will receive a reduced update to the IPPS standardized amount. The payment adjustment is applied cumulatively for each year that the eligible hospital fails to successfully attest.[9]

Adjustments for Eligible Professionals

Eligible professionals who qualify for the Medicare meaningful use program who do not successfully attest to the meaningful use program are subject to a payment adjustment beginning on January 1, 2015.[10] This payment adjustment is applied to the Medicare physician fee schedule amount for covered professional services. The payment adjustment begins at 1 percent per year and increases for every subsequent reporting period that an eligible professional fails to successfully attest and can climb as high as 5 percent per reporting period.

Adjustments for Critical Access Hospitals

Critical access hospitals that are not meaningful CEHRT users, and therefore failed to successfully attest, can anticipate a payment adjustment beginning in FY 2015. This payment adjustment is applicable to the critical access hospital's Medicare reimbursement for inpatient services during the cost reporting period during which the critical access hospital failed to successfully attest under the meaningful use program. The critical access hospital's reimbursement will be reduced from 101 percent of its reasonable costs to 100.66 percent of its reasonable costs in the first year it fails to successfully attest. Thereafter, for a cost reporting period beginning in FY 2016, the critical access hospital's reimbursement would be reduced to 100.33 percent of its reasonable costs and for a cost reporting period beginning in FY 2017 and each fiscal year thereafter, its reimbursement would be reduced to 100 percent of reasonable costs.[11]

Penalties Under the False Claims Act

A failed audit may also indicate a false attestation, and a false attestation could potentially be the basis for a claim under the False Claims Act. The False Claims Act imposes liability for a person who knowingly submits or makes a false record or statement to the government to get a false claim paid.[12] The damages and penalties are substantial and include civil monetary penalties and treble the amount of the government's damages.[13] It is reasonable to assume that payment of a meaningful use program incentive payment that must be returned because of a failed audit may expose the eligible provider to a False Claims Act claim. When an eligible provider attests, the attestation disclaimer notes that the attesting party certifies that the submitted information is true, accurate and complete and that the use of ''any false claims, statements, or documents, or the concealment of a material fact used to obtain a Medicare EHR Incentive Program payment, may be prosecuted under applicable Federal or State criminal laws and may also be subject to civil penalties . . . [A]nyone who misrepresents or falsifies essential information to receive payment from Federal funds requested by this form may upon conviction be subject to fine and imprisonment under applicable Federal laws.''[14] This language and the particular facts and circumstances surrounding the attestation could be interpreted as the necessary knowledge and interest required for a prosecutor to bring a False Claims Act cause of action against an eligible provider.

Penalties Under the Health Insurance Portability and Accountability Act

Eligible providers should also be mindful that failing certain meaningful use objectives can signify a HIPAA compliance failure. For example, eligible providers must conduct or review a security risk analysis in accordance with the requirements under the HIPAA administrative safeguards provisions at 45 C.F.R. § 164.308(a). If a meaningful use audit reveals that an eligible provider is out of compliance with the security risk analysis requirements, then the eligible provider may be subject to an investigation by the Department of Health and Human Services Office for Civil Rights. Recently, in May of 2014, two health care organizations agreed to pay monetary settlements of $3.3 million and $1.5 million to settle charges that they potentially violated HIPAA, which were partially based on allegations that

---

[8] *Payment Adjustments & Hardship Exceptions for Eligible Hospitals and CAHS*, CMG (August 2014), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/PaymentAdj_HardshipExcepTipsheetforHospitals.pdf.

[9] *Id.*

[10] *Payment Adjustments & Hardship Exceptions Tipsheet for Eligible Professionals*, CMS (August 2014), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/PaymentAdj_HardshipExcepTipSheetforEP.pdf.

[11] *Payment Adjustments & Hardship Exceptions for Eligible Hospitals and CAHs*, CMS (August 2014), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/PaymentAdj_HardshipExcepTipsheetforHospitals.pdf.

[12] 31 U.S.C. §§ 3729 – 3733.

[13] 31 U.S.C. § 3729(a).

[14] *Attestation User Guide For Eligible Professionals: Medicare Electronic Health Record (EHR) Incentive Program*, CMS (June 2014), 63, https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/EP_Attestation_User_Guide.pdf.

the providers had failed to conduct an accurate and thorough risk analysis.[15]

Frequent and Avoidable Missteps and Problems

To avoid frequently encountered missteps and problems that may arise within a provider's participation in the meaningful use program, providers would be well-advised to consider the following practical recommendations:

Confirm that your organization's CEHRT is both certified and complete. Eligible providers must have a ''Complete CEHRT.'' A CEHRT that is not a ''Complete CEHRT'' in accordance with the Office of National Coordinator standards and certification criteria may not meet the necessary functionality required to pass an audit.[16] Eligible providers should confirm that the CEHRT is documented on the certified health IT product list.[17]

Do not send protected health information to the meaningful use program auditor. Any documentation submitted during the audit should not contain protected health information, and eligible providers should take the necessary precautions so that any documentation from an audit complies with applicable HIPAA protections.

Beware of outdated meaningful use program documentation. CMS and the ONC continue to issue additional guidance and commentary regarding proper and appropriate documentation. Eligible providers should be conscious that any documentation used to support attestation is both current and properly maintained. Also, eligible providers should carefully weigh the accuracy and reliability of any information provided by third parties, including the CEHRT vendor.

Avoid failing to perform or properly document public health connectivity. The meaningful use program requires that an eligible provider use CEHRT to submit electronic data to immunization registries or immunization information systems and that actual submission according to applicable law and practice occurs.[18] This measure has been problematic for eligible providers because the test will be performed, but an adequate audit trail is not properly maintained demonstrating successful transmission. Eligible providers can request a letter from the appropriate state agency to validate the test date and that the information was submitted.

Avoid failing to properly review or conduct a risk analysis as required by HIPAA during the applicable reporting period and at each location. For both Stage 1 and Stage 2 of the meaningful use program, eligible providers are required to conduct or review a security risk analysis for each reporting period. Eligible providers continue to struggle with demonstrating that both a risk analysis was conducted or reviewed and, more importantly, that it occurred during the applicable reporting period. Eligible providers should track and document when a risk analysis is conducted or reviewed and any subsequent remediation efforts that are undertaken in response to such risk analysis.[19] Likewise, any documentation should include verification that each provider and location was included in the risk assessment. This likely requires advance planning for those eligible providers who provide services with CEHRT at facilities that are not directly under the control of the eligible providers' employers.

Beware of inconsistent denominators across multiple meaningful use program measures. An attestation that includes different denominators for similar measures is likely to raise suspicion. Eligible providers should confirm that all denominators are accurate, and, if the attestation includes different denominators, the eligible provider should be able to provide documentation to support any differences.

Eligible providers' implementation and use of CEHRT, bolstered by support from programs such as the Medicare and Medicaid meaningful use programs, is a key component in shaping the future of health care management, improvement and delivery. As technology continues to advance, eligible providers will have access to vast amounts of information through the development of a health information technology infrastructure that will enable them to better collaborate and improve cost, quality and efficiency. While current discourse regarding the Medicare and Medicaid meaningful use programs focuses primarily on the incentive payments available to eligible providers, providers who choose to utilize such incentive payments should be aware of the ongoing compliance requirements that the programs impose to avoid potentially running afoul of the program requirements or other applicable laws. Failure to prepare for, manage and document compliance, beginning with the submission of the eligible provider's attestation, could lead to a failed audit, which in turn may impose repayment obligations and other legal action or penalties on the provider. All eligible providers should review their policies and procedures to ensure that compliance with the meaningful use program requirements is appropriately documented and that a team of individuals is ready to respond in the event of an audit.

---

[15] U.S. Department of Health & Human Services, *Data breach results in $4.8 million HIPAA settlements*, HHS.gov (May 7, 2014), http://www.hhs.gov/news/press/2014pres/05/20140507b.html.

[16] *Standards & Certifications Criteria Final Rule*, Health IT.gov (April 9, 2014), http://www.healthit.gov/policy-researchers-implementers/standards-certifications-criteria-final-rule.

[17] *Certification Programs & Policy: Certified Health IT Product List (CHPL)*, HealthIT.gov (June 30, 2014), http://www.healthit.gov/policy-researchers-implementers/certified-health-it-product-list-chpl.

[18] *Step 5: Achieve Meaningful Use Stage 1: Immunization Registries Data Submission*, HealthIT.gov (Feb. 27, 2014), http://www.healthit.gov/providers-professionals/achieve-meaningful-use/menu-measures/immunization-registries.

[19] *Security Risk Analysis Tipsheet: Protecting Patients' Health Information*, CMS (December 2013), http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/SecurityRiskAssessment_FactSheet_Updated20131122.pdf.

   ISSN 1064-2137