The Medicare and Medicaid EHR incentive programs require providers’ demonstration of Meaningful Use (MU) of Electronic Health Records (EHRs) based on complex regulations that include an auditing and appeals program.

Participation in the programs requires healthcare professionals and hospitals to use more than 30 EHR technology functions defined as MU measures. These include functions intended to improve healthcare quality, efficiency and care coordination (e.g., computerized provider order entry), electronic prescribing and exchange of key clinical measures.

A brief history of the MU program

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act (ARRA), established Medicare and Medicaid incentive programs to promote adoption of EHRs. An EHR is classified in the law as a “computerized recordkeeping system that contains patients’ health-related information, including medical history.”

The federal program began making payments to professionals and hospitals in May 2011, and will continue to make incentive payments through 2016. Professionals can receive up to $44,000 each in incentive payments over the duration of the program. Hospital payments begin with a $2 million base amount adjusted by a number of hospital-specific factors, and gradually decrease over the program’s duration. Hospitals and eligible providers that don’t participate in the program will begin accruing reimbursement penalties in 2015.

State Medicaid agencies administer their own Medicaid EHR incentive programs and are responsible for
overseeing program integrity. States make incentive payments directly to healthcare practitioners and hospitals. The Centers for Medicare and Medicaid Services (CMS) provides enhanced federal financial participation to states for their EHR incentive programs. States are required to have an oversight plan to combat fraud, waste and abuse, including checking that health practitioners and hospitals are eligible for the incentive payments. CMS identified Medicaid EHR incentive program eligibility as an oversight priority for states’ Medicaid EHR incentive programs beginning in 2011.

**Auditing and oversight is a multi-agency approach**

CMS, the Office of the Inspector General (OIG), and the General Accounting Administration (GAO) all have a stake in the Meaningful Use program, including the audit process.

The MU program represents more than $30 billion that will be given to providers to develop and enhance patient care through EHR systems. In September, 2012, CMS extended the proposed MU program timeline through 2021. The Secretary of Health and Human Services may extend the program further.

**Self-certification**

CMS and the Office of the National Coordinator implemented the EHR incentive program by adopting a self-certification strategy whereby providers certify their Meaningful Use of certified EHR technology as part of an attestation process required to claim incentive payments. The goal of CMS is to verify the accuracy of the claims made by providers. CMS shared their priorities regarding the program early on in the MU process:

- All providers receiving incentive funds are subject to audit.
- A single deficiency in meeting a required MU measure will result in a finding of noncompliance, and CMS will move to recoup the entire incentive payment.
- Providers will be selected for audits based on a risk factor approach developed by CMS.
- CMS will evaluate the effectiveness of the audit strategy on an ongoing basis and modify the program as warranted.
- Federal and state audits have a different focus with state Medicaid agencies administering state audits of MU funds, primarily through eligibility checking, although state programs may vary; federal audits emphasize performance and compliance with the MU criteria.

**Incentive payment recoupment**

Officials at CMS will recoup an EHR incentive payment if an entity fails to comply with an audit request to produce documents or data needed to audit the validity of an EHR
You can and should play a key role in the organization’s MU program.

incentive payment. If the results of an audit indicate that the provider is not eligible for an EHR incentive payment because it does not meet one or more of the criteria, CMS will recoup the incentive payment.

The OIG, in a report released in November 2012, noted that an early assessment found that CMS faces obstacles in overseeing the Medicare EHR incentive program. The OIG’s Work Plan for 2013 includes MU. The OIG states in the Work Plan:

“We will review Medicare incentive payments to eligible health care professionals and hospitals for adopting electronic health records (EHR) and the Centers for Medicare & Medicaid Services (CMS) safeguards to prevent erroneous incentive payments.”

According to the work plan, the OIG will also assess CMS’ plans to oversee incentive payments for the duration of the program and actions taken to remedy erroneous incentive payments.

The GAO conducted an evaluation of the first year of the EHR incentive program and reported to Congress there were opportunities to improve processes to verify providers have met the requirements. The OIG recommended that CMS:

- Establish timeframes evaluating the effectiveness of its audit strategy
- Request more information from Medicare providers during the attestation process
- Evaluate the extent to which it should conduct more verifications on a prepayment basis
- Consider collecting MU attestations from Medicaid providers on behalf of the states

The implications of these studies and evaluations are clear. The focus is on auditing, improved auditing through an iterative and changing process, discovery of potential fraud and recoupment of payments where appropriate. Essentially, the results of the studies indicate the incentive program lacks a thorough accounting to ensure the funds go to those who actually achieve MU of EHRs.

The OIG has consistently warned providers of documentation pitfalls in the use of EHRs that can lead to False Claims Act violations. Two common problems include cloning:

- A clinician copies and pastes the same notes for several patients or for several visits for one patient into the record.
- Over-documentation can occur when an electronic system automatically copies information and includes it with documentation for each visit.

The OIG recommends that providers audit these areas to ensure documentation is accurate and that billing for services is appropriate.

You should be aware that attesting to completing a security risk assessment, if one has not been done, is also a potential false claim. The OIG may use the False Claims Act as an instrument for whistleblower or other lawsuits, based on the assumption that some providers will file false attestations.

Highlights of the 2014 Edition Standards and Certification Criteria (S&CC)

The Office of the National Coordinator for Health Information Technology’s role is the certification of EHR systems and standards requirements. The office released its 2014 Edition Standards and Certification Criteria that includes standards, implementation specifications and certification criteria for EHR technology.

The Standards and Certification Criteria redefines the meaning of Certified Electronic Health Record Technology (CEHRT) to improve certification efficiency, permit greater innovation on the part of providers and vendors, and to reduce regulatory burdens associated with operating and maintaining EHR technology.

The certification criteria now include consistent vocabulary, content exchange, transport, functional and security standards.

The test reports used for EHR technology certification must be made publicly available and EHR technology developers must follow price transparency practices related to the types of costs (i.e., one-time, ongoing, or both) associated with EHR technology implementation for MU. Providers should not hesitate to ask for this information when conducting reviews and due diligence on vendor products.
The certification criteria and process provide flexibilities for eligible providers and allow them to choose and customize the EHR technology that works best for them and their patients.

**The attestation process: auditing pitfalls**
To receive Medicare EHR incentive payments, providers must attest that they meet Meaningful Use criteria using certified EHR technology. Attestation is required at each stage of the MU program.

*All information submitted during registration, attestation and any subsequent validation and audit procedures must be backed up by auditable data sources or documentation.*

The attestation process requires “... demonstrated Meaningful Use of certified EHR technology during the EHR reporting period,” and “... documented evidence of a recent risk analysis, findings of the analysis and subsequent implementation of updates and corrections.”

Providers who receive MU funds must continue to meet these Security Rule Risk Analysis requirements:

- Perform a security risk analysis in accordance with the requirements of 45 CFR 164.308(a)(1)
- Implement security updates as necessary and correct identified security deficiencies as part of the provider’s risk management process

The goal is to protect electronic health information. Providers must continue to develop and implement remediation and action plans for addressing threats and vulnerabilities documented through the risk analysis process. Managing and mitigating risks is key to maintaining an effective privacy and information security program.

As new criteria are developed and included in the MU program, providers must enhance their security programs to offer more robust protection for confidential information and records.

Providers should review and update policies, train and re-educate staff on key issues and new threats associated with technology (smartphones, social media, etc.) and communicate privacy and security benefits to patients. Providers should update business associates on the Breach Reporting Rule roles and responsibilities and work with vendors to decrease the potential for breaches and mitigate breaches.

**Audit documentation requirements**
The audit program is one of the government’s tools to enhance compliance with the regulations, uncover fraudulent use of public funds and recoup monies that have been inappropriately received.

All information submitted during registration, attestation and any subsequent validation and audit procedures must be backed up by auditable data sources or documentation. Providers are required to retain documentation to support all attestations for no less than six years after each payment year.

Evidence of documentation may include:

- Computer screen shots showing required EHR technology functions were enabled during the reporting period
- Documents verifying a security risk assessment was conducted and mitigation plans put in place
- Documentation of patient volume, including those with paper records, for percentage-based measures with all patient denominators

The regulations indicate that in the event of an audit, at minimum, providers should have available electronic or paper documentation supporting their completion of the Attestation Module responses, including the specific information supporting each measure.

In addition, providers should have documentation to support the submission of clinical quality measures, including the specific information supporting each measure. Providers should also maintain documentation to support incentive payment calculations (e.g., data to support amounts included on the cost report used in the calculation). Providers should keep documentation at least six years following the date of attestation.
ONCHIT guidance

The Office of the National Coordinator for Health Information Technology published a Guide to Privacy and Security of Health Information in 2012. CMS takes privacy and security very seriously. Here are some notes from this guide that bear emphasis:

Do not register and attest for an EHR Incentive program until you have conducted your security risk analysis (or reassessment) and corrected any deficiencies identified during the risk analysis. Document these changes/corrections. Providers participating in the EHR audit program can be audited. When you attest to Meaningful Use, it is a legal statement that you have met specific standards, including that you protect ePHI.

For MU purposes, a risk analysis only needs to be done once per year, or when a major change occurs to your practice or electronic system, such as your decision to participate in a health information exchange (HIE).

You must perform a security review of your electronic health care system and correct any practice that might make your patients’ information vulnerable. A security update could be updated software, changes in workflow processes or storage methods, new or updated policies and procedures…

Providers attesting for the incentive programs should heed this advice. Failure to do so can result in significant problems and penalties later.

Regulatory requirements for auditing and appeals processes

CMS initiated audits of the attestation materials in 2012, through a contract with Figliozzi and Company, acting as CMS’ auditor for the program. While CMS has not stated this explicitly, it may be assumed the results of these audits will

---

### Exhibit 1

<table>
<thead>
<tr>
<th>Example of MU audit</th>
<th>Key areas of focus/information</th>
</tr>
</thead>
</table>
| Audit of Vendor Contract and/or Service Level Agreement (SLA) for EHR products and services | Signed/dated contracts, purchase orders, receipts for purchase or lease of certified EHR software or proof of service by hosted EHR software  
  - Documentation of expenses incurred in development, testing, maintenance, upgrades of EHR systems or modules  
  - Proof of payment and completion of consulting services (e.g., selection, acquisition, installation, setup of certified EHR technology; implementation of training programs; integration with clinical workflow; and completion of required interfaces)  
  - Purchase orders or receipts for computer hardware, software, and other devices required to operate the EHR system  
  - Proof of actual expenditures for testing of the EHR system  
  - Proof of actual expenditures for training the workforce on the EHR system |
| Security Audit of EHR Vendor |  
  - Vendor security policies  
  - Documentation of vendor security certification by approved accrediting body  
  - Documentation of technical testing (methods, results, recommendations) performed on systems housing EHR and confidential information for providers and maintained by a vendor  
  - Verification of security functionality included in the EHR system  
  - Test reports for technology certification  
  - Testing of key security provisions of system |
| Documentation Audit |  
  - Attestation documentation (e.g., screen prints, documentation backing up criteria, security risk assessment and mitigation plan)  
  - Calculations used to determine compliance with all criteria in the attestation process  
  - Review of online documentation system or paper records for MU process  
  - Committee/Work Group minutes and reports  
  - Other documentation pertinent to the MU program  
  - Coordination of documentation (responsible party, ongoing documentation, ease of retrieval, etc.) |
be used to develop more substantial audits with additional initiatives as the program progresses.

States are required to implement appeals processes for Medicaid providers receiving EHR incentive payments. Providers may appeal:

- The incentive payments amounts
- Provider eligibility determinations
- Demonstration of adopting, implementing and upgrading an EHR system
- Meaningful Use eligibility for incentives

A provider may challenge the state’s determination by submitting documents or data to support the provider’s claim.

**Opportunities for you to add value to the MU program**

You can and should play a key role in the organization’s Meaningful Use program. You should include audits of various aspects of the MU program in your annual audit plan. These will assist management in identifying and mitigating risks associated with the program, including reputational, financial, operational, security, compliance and enforcement risks.

Development and implementation of specific audits should be based on available resources, priorities and consistency with your annual audit planning process. The MU program will continue to be a primary component of an organization’s approach to Electronic Health Records for years to come. Internal auditors will need to determine which MU audits best serve their organizations and include them in each audit cycle.

Exhibit 1 suggests audits you can perform to add value to your organization’s MU program, along with some key areas of focus and information that can be included. The list is an overview of the possible areas you may choose to focus on. Additional audit areas may be added as the MU program evolves. NP