Protect your practice from Meaningful Use audit
What this white paper contains

- Introduction
- Audit is inevitable
- Handle audit swiftly
- Physicians have to take charge
- Avoid discrepancies
- Use certified EHR
- Documentation is key
- Do a security risk assessment
Introduction

The Centers for Medicare and Medicaid Services (CMS) has distributed more than $23 billion in Meaningful Use incentives and is moving closer to its budget of $27 billion. However, with the increase in the amount of incentive payments, there is a visible increase in Meaningful Use audits. Physicians across the country must gear themselves up for audits and prepare accordingly.

CMS has contracted Figliozzi and Co. to conduct the Medicare Meaningful Use audit program, however, the number of audits conducted so far is still a secret. People close to the matter say they have seen a spike in recent months in the frequency of auditing and that some physicians are not prepared when they are sent the audit letters.

These seven simple strategies will help guarantee a smooth, convenient and favorable audit for your practice.
Audit is inevitable

By anticipating the audit to take place before they attest it, physicians can work more on the preparation and consequently expect a favorable outcome.

As physicians are randomly chosen for audits, and no one can fully eliminate the risk of being audited, it is better to be prepared beforehand.

Several Meaningful Use experts suggest the retention of certain documents the auditors will demand. By grouping these documents in a single file, they can produce the documents instantly whenever audited, and are thus saving time and potential inconvenience.

Experts add that when the physician’s fulfillment of the Meaningful Use program participation is validated, and records of documentation, registration and attestation processes are maintained for at least six years, the physician will have a strong grounding when responding to the audit.

Handle audit swiftly

While the audit process requires fulfilling a long checklist, and can often be challenging and frustrating, altercations with the auditors should always be avoided.

Legal experts point out that the CMS is a proponent of paying out the money to promote Electronic Health Records (EHR) use.

While a maximum of 14 days are generally allowed for responding to an audit notice, gathering the documents required can be extremely time consuming and thus needs to be done on a priority basis (starting from the day the letter is received).
Additionally, these experts highlighted that presenting information to or engaging the auditors outside of the document exchange period results in penalties for the physicians for failing to provide the necessary documentation. Responding with only statements to particular document requests is another common mistake physicians make.

**Physicians have to take charge**

Numerous small practices assign the groundwork of Meaningful Use programs to practice managers. However, the physicians must keep checks on these managers to make sure, not merely assume, that the work is being done.

With the reputations of both the physician and practice at risk, it is better not to rely on assumptions.

**Avoid discrepancies**

The auditors have been assigned to identify discrepancies between information submitted in the attestation process and what was done in reality.

An emailed letter from Figliozzi informs the practice that it is being audited. A document request list accompanies this letter. Both prepayment and post-payment audits follow the same procedure and every physician being audited must present the same documents, classified according to these three categories:

- Evidence of certification of the EHR system used to satisfy Meaningful Use requirements.
- Proof of accurate quality measure, core, and menu objective data.
- Evidence of the performance of a security risk assessment and the presence of a corrective action plan.
Use certified EHR

Conformational documents from vendors specifying the EHR system version provided to the physician are necessary to satisfy the certification requirements required by auditors as several vendors may possess and provide older, uncertified versions of their EHRs.

A list of certified EHR products is present on the Office of the National Coordinator’s (ONC) website. Physicians need to keep an eye on any upgrades to their systems to ensure that these do not affect the practice’s certification status.
Documentation is key

According to several experts in the field, the data used in the registration and attestation of the Meaningful Use Program including the data generated by EHR reports and proof of all “yes/no objectives” must be presented in an auditable form.

Objectives requiring report generation (including numerators and denominators) must include support-documents validating the accuracy of the denominator and a report confirming the numerator’s convergence with the required threshold. Cross-checking with the practice management system’s patient population data could also be needed to attest the denominator’s accuracy.

The yes/no objectives deal with the functionality that is switched on (during the reporting period). Experts believe that physicians should use printouts of dated screenshots from their EHRs to validate that the function was on during the reporting period.

While practices need to only show that the required functions were turned on, it becomes all the more necessary for the practitioners to perform multiple checks over time throughout the reporting period to ensure that those functions are, actually, turned on.
Do a Security Risk Assessment

According to experts, security risk assessment is one of the requirements many physicians fail to meet.

While practices should have adopted risk analysis techniques as soon as the 2005 Health Insurance Portability and Accountability Act (HIPAA) Security Rule came into effect, many are still new to the concept, experts believe.

Apart from putting the physicians at risk of reimbursing the incentive money, neglecting the risk assessment process can also result in the U.S. Department of Health and Human Service’s Office for Civil Rights penalizing the physicians for HIPAA non-compliance.

The ever-evolving nature of risk assessment makes it extremely challenging for physicians to comprehend and to comply with as each change in practice, or every time new technology is endorsed, requires specific risk management provisions.
Nine Elements of a HIPAA Risk Assessment

The following pointers contain an outline of the risk assessment process:

1. **Scope of the analysis** – Any potential risks and vulnerabilities to the privacy, availability and integrity of ePHI (Electronic Protected Health Information).

2. **Data collection** – An organization must identify where the ePHI is stored, received, maintained or transmitted.

3. **Identify and document potential threats and vulnerabilities** – Identify and document any anticipated threats to sensitive data, and any vulnerabilities that may lead to leaking of ePHI. Anticipating potential HIPAA violations can help your organization quickly and effectively reach a resolution.

4. **Assess current security measures** – What kind of security measures are you taking to protect your data? From a technical perspective, this might include any encryption, two-factor authentication, and other security methods put in place by your HIPAA hosting provider.

5. **Determine the likelihood of threat occurrence** – Take account of the probability of potential risks to ePHI – in combination with #3 Potential Threats and Vulnerabilities, this assessment allows for estimates on the likelihood of ePHI breaches.

6. **Determine the potential impact of threat occurrence** – By using either qualitative or quantitative methods, assess the maximum impact of a data threat to your organization.
7. **Determine the level of risk** – HHS suggests taking the average of the assigned likelihood (#5) and impact levels (#6) to determine the level of risk. Documented risk levels should be accompanied by a list of corrective actions that would be performed to mitigate risk.

8. **Finalize documentation** – Write everything up in an organized document – HHS doesn’t specify any format, but they do require the analysis in writing.

9. **Periodic review and updates to the risk assessment** – It’s important the risk analysis process is ongoing – one requirement includes conducting a risk analysis on a regular basis. While the Security Rule doesn’t set a required timeline, HHS recommends organizations conduct risk analysis whenever your practice implements or plans to adopt new technology or business operations.
About CureMD

CureMD is the leading provider of Cloud-based EHR, Practice Management and Medical Billing Services to transform the administrative and clinical operations of healthcare organizations of all sizes. Our award winning solutions simplify decision making, streamline operations and ensure compliance with industry standards and best practices – ultimately saving time and effort to maximize value and returns.

For more information, call (212) 852 0279 ext. 384 or email to media@curemd.com.