Checklist and Related Guidance for Meaningful Use Audits

This checklist was prepared by Jill M. Girardeau, Partner, Womble Carlyle Sandridge & Rice, LLP and Dina Marty, Counsel, Wake Forest Baptist Medical Center.

Because an audit relating to the Medicare or Medicaid EHR Incentive Program may focus on any number of issues, it is not possible to identify each and every document that may be requested by an auditor. In addition, this checklist is based on specific experience with specific auditors; different auditors may have different requests, requirements, and standards. However, this checklist may be useful in gathering and maintaining documentation supporting an attestation for a Medicare or Medicaid EHR Incentive Program payment.

Links to websites were accurate as of the date these materials were prepared (January 16, 2014). We cannot guarantee that the links provided in this document will continue to direct the reader to the specific materials referenced.

This checklist does not constitute legal advice.

General Guidelines

- An audit can be a pre-payment or a post-payment audit and may be a desk audit or a field (on-site) audit. During a field audit, auditors may require a demonstration of the Certified EHR.

- An audit can occur anytime in the six-year period following attestation. A provider that has attested under the Medicare or Medicaid EHR Incentive Program should keep all audit documentation, including the actual attestation submitted, for at least six years. The documentation should be maintained in a secure (but accessible) fashion.

- Documentation supporting hospital payment calculations should follow current retention requirements.

- Figliozzi and Company is performing audits under the Medicare EHR Incentive Program. States arrange for audits under the Medicaid EHR Incentive Program. On behalf of CMS, Figliozzi and Company will audit hospitals that are eligible under both the Medicare and Medicaid EHR Incentive Programs.

- CMS has provided sample audit letters here:

- A provider may have as little as two weeks to respond to an audit request. All documentation and information used for attestation (and any other helpful documents)
should be maintained in an audit file that is readily available so as to avoid a rush in pulling together requested documentation.

- For Medicare EHR Incentive Program audits, information requested can be provided by mail or by uploading to a secure portal provided by auditors.


- Payments received under the Medicare and Medicaid EHR Incentive Programs are subject to federal laws governing fraud and abuse, so providers who submit a fraudulent attestation may be subject to sanctions.

- If a provider is found to be ineligible for an incentive payment under the Medicare or Medicaid EHR Incentive Program, any payment already received will be recouped from the provider.
  - A provider who has failed an audit under the Medicare or Medicaid EHR Incentive Program does have appeal rights. [http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Appeals.html](http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Appeals.html)
  - When submitting an appeal relating to a failed audit, a provider can choose not to repay at that time. However, if the appeal is denied, the incentive payment must be repaid and additional interest may be charged.

**Supporting Documentation**

- **Proof of Certified EHR**
  - Certifying bodies (like CCHIT and Drummond Group) certify specific versions of EHRs. Make sure that the version of the EHR being used is a version that is a Certified EHR.
  - Ensure that you provide a CMS EHR certification ID number for your Certified EHR during attestation. This number is available on the Certified Health IT Product List ([http://onchpl.force.com/ehrcert/CHPLHome](http://onchpl.force.com/ehrcert/CHPLHome)). More information on the CMS EHR certification ID number is available here: [http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html](http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Certification.html)
  - For audit purposes, a license agreement with or purchase order from the Certified EHR vendor may suffice to prove the use of a Certified EHR. However, any such license agreements or purchase orders may have confidentiality provisions that prohibit them from being shared with others, even auditors. Review any agreements with or documentation from the Certified EHR vendor prior to sharing with auditors and consult with legal counsel if necessary. Also, if needed, consult with the Certified EHR vendor as to what documentation is appropriate to
provide to auditors. Some vendors provide license summaries or similar documentation for audit purposes.

- Consider the Medicare and Medicaid EHR Incentive Programs prior to implementing an upgrade of a Certified EHR. Will there be a timeframe during a reporting period when a Certified EHR is not being used?

- CMS has stated that an EHR certified for other CMS programs may not necessarily be certified for the Medicare and Medicaid EHR Incentive Programs. Only EHRs certified for the Medicare and Medicaid EHR Incentive Programs satisfy the requirement that a provider use a “Certified EHR.”

**Source Document**

- The source document, which is usually a report from the Certified EHR, should include the following:
  
  - Numerators and denominators for all percentage-based measures;
  
  - Time period the report covers; and

  - Evidence to support that the report was generated for a specific provider.

Auditors have questioned reports from Certified EHRs that do not specifically identify the provider on each page. Auditors have also questioned reports that do not include the Certified EHR logo, the version number, and the date on each page. Review the reports generated by your Certified EHR and contact your Certified EHR vendor with any questions.

- Clinical quality measures must be reported from the Certified EHR, so maintain a report to validate the clinical quality measures reported.

- Determine whether the Certified EHR you are using can generate reports for prior time periods. If not, a report must be generated for the EHR reporting period and maintained in a reproducible format.

- Anomalous data will be scrutinized. For example, not all percentage-based measures use the same denominator, so attesting with the same denominator in all percentage-based measures may result in an audit. Similarly, different denominators in the percentage-based measures that do use the same denominator may result in an audit as well. Attesting to 100% for each percentage-based measure is also problematic. If all physicians in a practice attest with the same percentages, payments to those physicians are likely to be questioned. Scrutinize the numbers before attesting.
**Documentation of Yes/No Measures**

- Screen shots must be from the Certified EHR and must be *from the reporting period*. Take screen shots before the end of the reporting period and maintain them in case of an audit.

- Screen shots should show date, provider, and name and vendor of the Certified EHR and the version number. To the extent possible, redact patient-specific information before providing to auditors. We note, however, that certain auditors (especially those auditing under the Medicaid EHR Incentive Program) may request certain types of patient-specific information.

- If screen shots were not obtained during the reporting period, work with your Certified EHR vendor to determine how to obtain documentation showing that the yes/no measures were met during the reporting period. Can the information be obtained from audit logs? Does the vendor have any information demonstrating when a particular functionality was turned on or off?

- Some Certified EHR vendors have implemented contractual restrictions on the provision of screen shots to auditors. Review the relevant license agreements, purchase orders, etc. to determine whether any contractual restrictions exist and consult legal counsel if necessary.

**Security Risk Analysis**

- Meaningful use requires a provider to conduct or review a security risk analysis as required by the HIPAA security rule.

- The security risk analysis must factor in the version of the Certified EHR that is being used for meaningful use purposes but must address other security issues as well, not just the Certified EHR.

- CMS and OCR have provided guidance on the security risk analysis requirement:

- CMS and OCR have confirmed that a security risk analysis must be conducted during each Stage 1 and Stage 2 reporting period. A change in Stage 2 requirements means that the security risk analysis must address the encryption and security of data at rest.
Documentation of Exclusions

- A report from the Certified EHR showing a zero denominator for specific measures may suffice as documentation of an exclusion. For example, if immunizations are not part of an Eligible Provider’s practice, a report showing a zero denominator could satisfy an auditor’s request. However, it may also help to document the reason that the Eligible Provider does not provide any immunizations.

- Some exclusions are not dependent on denominators. For example, if the relevant health department did not accept electronic submissions of reportable lab results during the reporting period, an auditor may request documentation that electronic submission was not available. Many health departments have included this information on their websites or otherwise provided confirmation regarding their ability or inability to accept electronic transmissions.

Documentation of Transmissions

- CMS has provided examples of documentation related to transmissions that should be maintained for audit purposes:
  
  - Dated screenshots from the Certified EHR system that document a test submission to an immunization registry or public health agency and show the result (i.e., successful or unsuccessful). The documentation should include evidence to support that it was generated for that specific provider’s system.
  
  - A dated record of successful or unsuccessful electronic transmission (e.g., screenshot from another system, etc.). This record should include evidence to support that it was generated for that specific provider.
  
  - A letter or email from an immunization registry or public health agency confirming the receipt or failure of receipt of the data submitted electronically. The letter or email should include the date of the submission, the name of the provider and the registry or agency, and the result of the test (i.e., successful or unsuccessful).

- If you plan to use an intermediary (like a health information exchange) to submit public health data, ensure that the use of the intermediary will still allow you to meet the meaningful use objectives. The following FAQs from CMS and ONC may be helpful:
  
  
  - [http://www.healthit.gov/policy-researchers-implementers/18-question-09-10-018](http://www.healthit.gov/policy-researchers-implementers/18-question-09-10-018)
To this point, our experience has been that auditors have not focused heavily on the transmission requirements, as many immunization registries and public health agencies were not prepared to receive the information. We believe that focus on the transmission requirements will likely increase going forward.

➢ Attestation

- Along with all the other types of documentation discussed here, maintain a copy of the actual attestation that was submitted.

- Also, make sure that whatever contact information provided during attestation (for example, an email address) is in working order and is being monitored. We have experienced several instances in which an email address is not being monitored and auditor communications are not read in a timely manner.

➢ Medicaid Considerations

- Audits under the Medicaid EHR Incentive Program vary by state. Here is state contact information: [https://www.cms.gov/apps/files/statecontacts.pdf](https://www.cms.gov/apps/files/statecontacts.pdf)

- Audits under the Medicaid EHR Incentive Program may focus on patient volume calculations. One representative of a state Medicaid program has said that multiple attempts to identify a 90-day period to establish patient volume may lead to an audit.

- Those providers with no history of providing services to Medicaid beneficiaries prior to the Medicaid EHR Incentive Program are also more likely to be audited.

- Based on our experience, documentation sufficient to demonstrate Adoption, Implementation, or Upgrade varies by state:
  - Some Medicaid representatives have said that demonstration of a financial or legal commitment for adoption of a Certified EHR will suffice and that no actual installation is required. Documentation may include an executed purchase order or agreement even if no payments to the Certified EHR vendor have been made.
  - Other Medicaid representatives have said that proof of installation is required. This proof may include evidence of costs associated with staff training and support during implementation or evidence of staff training on the Certified EHR. For an Eligible Hospital, a cost report showing implementation expenses relating to a Certified EHR may suffice.

Additional Suggestions

➢ Communicate with Auditors. Work with and communicate with auditors. If you cannot meet a deadline, let the auditors know as soon as possible. If you have any questions about the information being requested, ask the auditors for clarification.
Other Requests. Some providers have found that their financial auditors request information regarding the Medicare and Medicaid EHR Incentive Programs when performing a financial audit of the provider. For example, the financial auditors may want to confirm that the provider is actually entitled to payments from the Medicare or Medicaid EHR Incentive Program when determining whether the inclusion of incentive payments in the provider’s budget is reasonable.