Sample Checklists for Preparing and Responding to Audits of Electronic Health Records

These checklists should help providers prepare for an electronic health record (EHR) system internal or external audit. The checklists address how to respond to auditors during the audit, and how to follow up after the audit. The items included in the checklist should be typical components of internal training to prevent EHR fraud, waste, and abuse.

Reasons for EHR Audits

Regulatory agencies or integrity contractors may audit EHRs as part of a regular compliance program or because of random or deliberate selection. As part of their overall compliance program, providers should perform periodic internal and external audits with the objective of testing whether they are meeting compliance standards.[1, 2] Regulatory agency external audits can be part of an effort to measure, correct, and prevent improper payments and strengthen the integrity of the claims and payment process. Since EHRs are an integral part of the claims and payment process, auditors will review the EHR data and the audit log. Additionally, since incentive payments for adoption of EHR systems require meaningful use,[3] auditors may want to examine whether the provider demonstrated meaningful use.

For more information about physician and other health care professional audits and the roles played by regulatory agencies and contractors in them, watch the presentation, "Medicare and Medicaid Reviews, Audits, and Investigations: A Primer for Physicians and Other Health Care Professionals," posted to https://www.youtube.com/watch?v=y0QfKlXm1oM on the Centers for Medicare & Medicaid Services (CMS) YouTube channel.

Audit Notification

Provider audits generally start with a notice to the provider from the entity assigned to conduct the audit. When the administrator of a provider's EHR system receives notice an entity will audit the EHR data and log, the administrator should prepare and take certain steps. Usually the notice of an audit, whether internal or external, will contain the following information and associated requests:

- Why the audit is taking place;
- Who will perform the audit;
- What will be audited, or, the "scope" of the audit;
- Which records to provide, or a list of requested records to choose from; and
- Where the auditor will do the work: on-site or off-site.

Prepare for the Audit

The provider will have questions, and the answers to those questions will help them participate in the audit. If the provider does not have answers by the initial notice, they can ask questions as they prepare for the audit. The audit will move faster and will be more effective if the provider is better informed. Common questions include:

- Does the auditor want to see paper printouts of EHRs or have access to the EHR system, to the EHRs in a stand-alone electronic format, or a combination?
- What is the deadline for audit completion?
- Who is the auditor's single point of contact in the provider's office ("Lead")?
- What standards will the auditor apply to EHRs and why?

After a provider receives notice of an audit, they may use the Sample Checklist 1. Provider Audit Preparation to help prepare. This checklist does not necessarily cover all items. Additional items may be included, depending on the type and scope of the audit. As each question is addressed, place a check in the column next to the question, and be sure to complete the entire checklist in preparation for the audit.

Sample Checklist 1. Provider Audit Preparation

Item addressed	Check for Yes
Designate the Lead who will work with the auditor.	☐ Yes
Notify the auditors and staff who the Lead is.	☐ Yes
Designate staff to assist the Lead:	☐ Yes
Assemble an audit response team that includes persons with responsibility for information technology, including the EHR system, and operations, including budgeting, finance, compliance, and clinical.	☐ Yes
Assign staff responsibilities for responding to auditor requests for information or access to documents.	☐ Yes
Assign staff responsibilities for documenting auditor requests and responses to the auditor.	☐ Yes
Identify and assemble all policies and procedures related to the use of the EHR system.	☐ Yes
Document the internal EHR monitoring and auditing process currently in place.	☐ Yes
Document actions taken to follow up on identified incidents and the outcome of those actions.	☐ Yes
Determine if there are other items to add to this checklist due to the type or scope of the audit.	☐ Yes

Review the Audit Process and Seek Clarification

The Lead and response team should familiarize themselves with the general audit process, examine information available about the impending audit, and identify areas that require clarification.

The nature and timing of each EHR audit will vary somewhat, depending on the scope and objectives of the audit. In general, the audit process may include:

- Conducting an audit kickoff meeting;
- Selecting or identifying a sample of EHRs;
- Analyzing the sample to identify suspected instances of noncompliance with the law or with provider policy;

- Analyzing instances of noncompliance to determine cause, effect, and potential remedies;
- Communicating analysis and results to the provider, often informally during the course of the audit, and in the form of a draft report;
- Holding an exit conference to review and discuss preliminary findings, conclusions, exceptions, and recommendations;
- Giving the provider an opportunity to respond to the auditor's findings in writing;
- Delivering a draft written audit report to the provider;
- Incorporating the provider's responses to the draft in the final report, and delivering the final report to the provider;
- Imposing a corrective action plan and recovering overpayments if the auditor is a governmental agency or contractor;
- Imposing any applicable civil penalties if the auditor is a governmental agency; and
- Referring suspected fraud to law enforcement.

Follow-Up on the Audit Findings

The provider audit response team meets to discuss the final report and the items to address. The provider must return any overpayment identified by the audit within 60 days of the date of identification. Failure to do so may make the overpayment a false claim,[4] which could subject the provider to serious consequences under the civil False Claims Act, including administrative penalties,[5] treble damages,[6] and exclusion from the Medicare and Medicaid programs.[7]

If fraud is involved in the overpayment, the provider should consider using the Self-Disclosure Protocol established by the U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG). The protocol is posted to http://oig.hhs.gov/compliance/self-disclosure-info on the HHS-OIG website.

Use the Sample Checklist 2. Addressing Audit Findings to assist with tracking the follow-up action. As each action is completed, place a check next to the action.

Sample Checklist 2. Addressing Audit Findings

Actions to be taken by the audit response team	Check for Yes
Review the contents of the final audit report and discuss the findings.	☐ Yes
Identify areas of weakness (for example, flaws in EHR software; misuse of EHR features or capabilities; or weakness in policies, training, or auditing and monitoring).	☐ Yes
Designate staff responsible for developing a corrective action plan to address each of the comments and findings.	☐ Yes
Review and implement the corrective action plans that address each comment or finding.	☐ Yes
Set dates for completing each item.	☐ Yes
Establish a plan to monitor and audit to determine the effectiveness of the changes.	☐ Yes

Following an external audit, it is good practice to add the areas of risk found to your internal monitoring plan. This practice allows for monitoring the effectiveness of the corrective actions implemented because of the external audit. For more information on audits, refer to the "Conducting Internal Monitoring and Auditing" job aid posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the CMS website.

To see the electronic version of these checklists and the other products included in the "Electronic Health Records" Toolkit posted to the Medicaid Program Integrity Education page, visit https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html on the CMS website.

Follow us on Twitter #MedicaidIntegrity

Reference

1 Centers for Medicare & Medicaid Services. Medicare Learning Network. (2014, June 26). Affordable Care Act Provider Compliance Programs: Getting Started Webinar (Slide 27). Retrieved April 13, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNEdWebGuide/Downloads/MLN-Compliance-Webinar.pdf

2 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. 65 Fed. Reg. 59434, 59437. Retrieved April 13, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

3 Meaningful Use Objectives and Measures for EPs, Eligible Hospitals, and CAHs for 2015 through 2017. 42 C.F.R. § 495.22. Retrieved April 13, 2016, from http://www.ecfr.gov/cgi-bin/text-idx?SID=19c94ecb651c5a4eea05acbc96428773&mc=true&node=se42.5.495_122&rgn=div8

4 Social Security Act § 1128J(d). Retrieved April 13, 2016, from https://www.ssa.gov/OP_Home/ssact/title11/1128J.htm

5 Administrative Remedies for False Claims and Statements, 31 U.S.C. §§ 3801–3812. Retrieved April 13, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2010-title31/pdf/USCODE-2010-title31-subtitleIII-chap38.pdf

6 False Claims, 31 U.S.C. §§ 3729–3733. Retrieved April 13, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2010-title31/pdf/USCODE-2010-title31-subtitleIII-chap37.pdf

7 Social Security Act § 1128. Retrieved April 13, 2016, from https://www.ssa.gov/OP_Home/ssact/title11/1128.htm

Disclaimer

This checklist was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This checklist was prepared as a service to the public and is not intended to grant rights or impose obligations. This checklist may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

June 2016