Job Aid

Sample Checklist for Manual Review of Electronic Health Records

The security and integrity of documentation within an electronic health record (EHR) is important to the quality of care provided, demonstrates compliance with State and Federal law, and supports payment for services. Therefore, every entity that uses EHRs should have an established format and process for internal review. The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) recommends that a compliance plan include ongoing monitoring.[1] While software exists that will help with internal monitoring of EHRs, it may not be affordable for smaller provider entities. Software also may not identify misuse of some features that may lead to fraud, waste, abuse, and improper payments. This job aid should assist individual and small group providers, billing staff, and others internally review EHRs to identify issues for further investigation and corrective action.

An internal records review should include four steps. Providers need to complete all of the steps to ensure a complete review. These steps are:

1. Define the review objectives.
2. Develop a review methodology.
3. Select the elements for review.
4. Analyze the findings and identify solutions.

1. Define the Review Objectives

HHS-OIG guidelines recommend an annual review of standards and policies used by administrative staff to ensure they are current and complete. Additionally, the guidelines recommend an annual review of medical records by billing and clinical staff to ensure compliance.[2] The first step in any EHR review process is defining the objectives of the review. These objectives may include existing EHR-related program integrity vulnerability areas identified through risk analysis, fraud detection software, or claims processing experience (for example, a high number of rejected claims).

2. Develop a Review Methodology

Develop a consistent methodology for selecting records for review. Select a random sample of between five and ten EHRs per Federal health care program or per provider.[3] Many EHR systems can generate a list of current patients for selecting and tracking records for review. As monitoring is an ongoing activity, providers can divide the number of records for review into smaller amounts so that the goal is achievable over a period while still providing a thorough review. For example, it may be easier to integrate reviewing three records per week over a 6-month period into the workflow of a small practice than reviewing 60 records over a 2-week period every 6 months.

3. Select the Elements for the Review

Internal policies and standards, Federal and State regulations and guidance, and best practices address several program integrity areas that will globally apply to all of the EHRs you review. These areas include verification that:

- EHR system security features, including the audit log, access restrictions, and alerts and warnings, are appropriately enabled;
- EHR documentation features, such as templates or macros, are appropriately used;
- EHR capabilities that facilitate documentation, such as copy and paste, are appropriately used; and
- EHRs do not include intentional deception or misrepresentation such as over-documentation, fabrication, or false attribution that results in an unauthorized benefit.[4]

Selection of the list of elements should help to identify program integrity issues that may require a more focused review.[5] Including between six and eight elements makes it manageable. Sample Checklist 1. Electronic Health Record Review includes a column of suggested elements to review to protect the integrity of the EHR and prevent improper payments. It also includes a column of items that are potential red flags. The elements and potential red flags on the checklist are not comprehensive. The remaining columns on the checklist include an example and space for review of two EHRs. Place a check in the column if you reviewed the element, the element meets the criteria, and no findings require further action. Place an X in the column if you reviewed the element and the element does not meet the criteria, and then briefly identify the reason so further action is taken.

Sample Checklist 1. Electronic Health Record Review

Elements[6]	Potential Red Flags	EHR Example	EHR 1	EHR 2
Accuracy: Validation of information in notes.	• No validation of dictated, scribed, or voice-to-text notes; • Multiple authors of one note with only one author identified; or • Authorization by another provider not associated with the patient.	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Accessibility: Patient or authorized provider or staff member can access the information.	• Multiple instances of unauthorized access when a patient is a well-known person (for example, a VIP, employee, or relative of employee); or • Patient notification of concern that a note does not reflect services provided.	☐ Yes ☒ No If No, explain: Patient is known as local politician. EHR accessed unnecessarily by staff.	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Comprehensiveness: Information meets requirements.	• Instances information does not support medical necessity for services; or • Instances documentation is auto-populated without clarification of diagnosis and treatment specific to the patient's condition.	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Consistency: Information is consistent throughout the record. Note: It is appropriate for diagnoses and treatment to change.	• Six months of notes that state a patient just had a baby; or • One note in the record states a patient is deaf, but is nowhere else in the patient record.	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:

Sample Checklist 1. Electronic Health Record Review (continued)

Elements[6]	Potential Red Flags	EHR Example	EHR 1	EHR 2
Currency: Most current information is contained in the notes.	• Every visit notes the same vital statistics or labs. Additional information brought forward is clearly identified as such.	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Definition: Specific meaning of a data element	• Clarify reason for collecting the data, what the data means, and how you will use the data (for example, make sure to clearly define the difference between race and ethnicity).	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Granularity: Level of detail for defining the data	• Requires varying levels of granularity depending on type of data	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Precision: If auto-populated text is used, enough free text is added to clearly describe patient treatment/ orders without over-documenting.	• Over- or underdocumentation	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Relevancy: Information in notes should be relevant and necessary.	• Additional text added to indicate a higher level of care was provided; or • Contains a large amount of unnecessary information.	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:
Timeliness: Documentation is entered at the end of a patient encounter and is validated in a timely manner.	• Date note is entered or authorized does not coincide with date of patient visit; or • Validation of entry does not coincide with entry of dictated or scribed notes.	☒ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:	☐ Yes ☐ No If No, explain:

4. Analyze the Findings and Identify Solutions

After reviewing the selected records, analyze any findings to determine whether to investigate further and identify any actions to take. For example, if an error found resulted in an improper payment by a Federal health care program, that payment is an overpayment. The provider must report and return the overpayment within 60 days of its discovery. Failure to do so may expose the provider to liability under the False Claims Act.[7]

Start by identifying the findings in each element area and the possible causes and effects of the errors. Then identify changes that can eliminate future errors. "Finding 1" in the next section provides an example of this process. It used the findings identified in the EHR Example column of the Electronic Health Record Review Checklist.

Finding 1 (from EHR Example column): EHR accessed unnecessarily by staff.

Expectation: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) created Standards for Privacy of Individually Identifiable Health Information, known the Privacy Rule.[8] Since EHRs contain individually identifiable health information, providers and others maintaining these records must comply with the Privacy Rule.

Error: Unauthorized staff accessed the patient's EHR. The patient is a local VIP.

Possible Solutions: The provider could implement the following to eliminate future unauthorized access:

- Contact the person designated for compliance to perform an internal investigation;
- Implement disciplinary action as required by established policies;
- Review and update security policies as necessary; and
- Implement staff training and education on security policies and Federal rules.

Providers and others can play a significant role in protecting the integrity of the information in EHRs. In addition to findings in individual EHRs, look for common errors and identify methods to address these trends. For example, look for over- or underdocumentation; inconsistencies in notes, including the same entry for multiple visits; or nonvalidation of dictated notes. Use these common errors as examples to educate staff on appropriate use of EHR features and capabilities and provide examples of good practice.

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

Follow us on Twitter #MedicaidIntegrity

References

1 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Physician Practices. 65 Fed. Reg. 59434, 59436. Retrieved April 6, 2016, from http://oig.hhs.gov/authorities/docs/physician.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. Step One: Auditing and Monitoring. 65 Fed. Reg. 59434. Retrieved April 6, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

3 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. Step One: Auditing and Monitoring. 65 Fed. Reg. 59434. Retrieved April 6, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

4 Association of American Medical Colleges. AAMC Compliance Officers' Forum. (2011, July 11). Electronic Health Records in Academic Medical Centers Compliance Advisory 2. Retrieved April 6, 2016, from https://www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf

5 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). OIG Compliance Program for Individual and Small Group Practices. Step One: Auditing and Monitoring. 65 Fed. Reg. 59434. Retrieved April 6, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

6 American Health Information Management Association. (2015, October). Data Quality Management Model (2015 Update). Retrieved April 14, 2016, from http://library.ahima.org/PB/DataQualityModel

7 Social Security Act § 1128J(d). Retrieved April 6, 2016, from http://www.ssa.gov/OP_Home/ssact/title11/1128J.htm

8 45 C.F.R. pts. 160, 164. Retrieved April 6, 2016, from http://www.ecfr.gov/cgi-bin/text-idx?SID=1a6fd6d86be254e4c2011ad1d0045ba5&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl

Disclaimer

This job aid 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 job aid was prepared as a service to the public and is not intended to grant rights or impose obligations. This job aid 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