Implementing the CMS Toolkit for EHRs in your Practice

Jill Young, CPC, CEDC, CIMC
Young Medical Consulting, LLC
East Lansing, Michigan
Disclaimer

This material is designed to offer basic information for coding and billing. The information presented here is based on the experience, training, and interpretation of the author. Although the information has been carefully researched and checked for accuracy and completeness, the instructor does not accept any responsibility or liability with regard to errors, omissions, misuse, or misinterpretation. This handout is intended as an educational guide and should not be considered a legal/consulting opinion.
Causes of Improper Payments

- Not all improper payments are fraud, but all payments made due to fraud schemes are improper.
- The Centers for Medicare & Medicaid Services is targeting all causes of improper payments:
  - From honest mistakes to intentional deception.
- Most common error is insufficient documentation.
Use of Electronic Health Records

- In 2014
  - 95% eligible hospitals registered to participate in EHR incentive program
- 2010 to 2013
  - Hospital use
    - ↑ from 15% to 80%
  - Physician use
    - ↑ from 25% to 50%
Use of Electronic Health Records

- Increase in concern
  - Potential for fraud, waste, and abuse
  - Loss of documentation integrity
    - Could lead to compromised patient care
Definition Fraud & Abuse

• FRAUD
  • When someone intentionally deceives or makes misrepresentations to obtain money or property of any health care benefit program

• ABUSE
  • When health care providers or suppliers perform actions that directly or indirectly result in unnecessary costs to any health care benefit program

The Primary difference between Fraud and Abuse is Intention
Toolkit

• Addresses common EHR system features and methods which, if used inappropriately, could compromise the integrity of Federal health care programs by facilitating fraud, waste, abuse, and improper payments.

• Covers some program integrity tools and techniques that can help providers and others to recognize, report, and prevent such activities.

• [https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html](https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html)
Electronic Health Records

• Program integrity depends on consistent incentives for better patient outcomes within a context that avoids over- or underutilization of services.

• Requires effective, ongoing program management and monitoring.
Electronic Health Records

- An EHR is a digital version of a patient’s paper chart

- EHRs are real-time, patient-centered records that provide information instantly to authorized users.

- EHRs contain patients’ medical and treatment histories
  - Data from ALL clinicians involved in patient’s care

- EHR systems are built to go beyond standard clinical data and can provide a broader view of a patient’s care.
Electronic Health Records

- EHR data “can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization”
  - per National Alliance for Health Information Technology

- Information moves with the patient—to the specialist, the hospital, the nursing home, the next state or even across the country

- EHR’s have the ability to share medical information among stakeholders
  - Also to have a patient’s information follow them through out their care journey

- EHRs are designed to be accessed by all people involved in the patients care—*including the patients themselves.*
EHR vs EMR

• EHRs should not be confused with electronic medical records (EMRs).

• EMRs are created and accessed within a single medical practice or health care organization, while EHRs are designed to be used by multiple entities.
Electronic Medical Records

• An EMR contains the medical and treatment history of the patients in one practice.

• EMRs have advantages over paper records; they allow clinicians to:
  • Track data over time
  • Easily identify which patients are due for preventive screenings or checkups
  • Check how their patients are doing on certain parameters—such as blood pressure readings or vaccinations
  • Monitor and improve overall quality of care within the practice
Electronic Medical Records

- A digital version of the paper charts in the clinician’s office.

- Information in EMRs doesn’t travel easily *out* of the practice
  
  - May need to be printed out and delivered by mail to specialists and other members of the care team

- Not any better than paper
• Health Insurance Portability and Accountability Act of 1996 (HIPAA)
  • Authorized the Secretary of the U.S. Department of Health and Human Services to create a rule that protects the security and privacy of individually identifiable health information.

• Privacy Rule
  • EHRs contain such health information
  • Providers maintaining these records must comply with the privacy and security requirements Rule.
Health Information Technology for Electronic and Clinical Health Act (HITECH)

- Promotes using health information technology to improve health care quality, safety, and efficiency.
- Sought to bring about widespread EHR adoption by 2014
Goals of the Act include the development of a nationwide health information technology infrastructure that:

- Allows for the electronic use and exchange of information
- Ensures security of patient health information
- Improves health care quality, and reduces medical errors and health disparities
- Reduces health care costs
- Provides appropriate information to help guide medical decisions
- Improves coordination of care among different providers
- Promotes early detection, prevention, and management of chronic diseases
Health Information Technology for Electronic and Clinical Health Act (HITECH)

• HITECH Act established the health information technology certification program and the Medicare and Medicaid EHR incentive programs

  • To encourage standardization of EHR content, systems, and interoperability

• To receive the incentive payments must adopt certified EHR technology and must show increasing levels of meaningful use of the technology
Laws

• Laws exist to punish those who seek to compromise the integrity of EHRs or use EHR systems to perpetrate Federal health care fraud include:

  • False Claims Act
  • Health Care Fraud Statute
  • Criminal provisions of HIPAA
  • Civil Monetary Penalties Law
  • Exclusion provisions of the Social Security Act
Laws

• If Fraud is Committed
  • Subject to civil monetary penalties
  • Exclusion from participation in Federal health care programs
  • Criminal fines
  • Imprisonment
Laws

• Patient Protection and Affordable Care Act of 2010
  • Increased criminal penalties for health care offenses involving losses of $1 million or more
  • Clarified that specific intent to violate the law is not required for conviction under the Health Care Fraud Statute
  • Payments to providers must be suspended when there is a reasonable suspicion that they have engaged in fraud
Guidance from OIG

• Issued several reports dealing with EHRs
  • Each EHR system’s audit log automatically records changes in EHRs
    • Capturing data elements, such as date, time, and user stamps, for each update to an EHR
    • Recommended the audit log be turned on so that data regarding all such changes can be captured
    • Outside auditors should use the logs to support investigations of potential fraud
Definitions

• Copy and Paste
  • Selecting data from one location and reproducing it in another; also called “cloning”, “cookie cutter”, “copy forward”, and “cut and paste.”

• Clinical plagiarism
  • Occurs when a physician copies and pastes information from another provider and calls it his or her own
Copy & Paste

• Health care professionals have stated that copying and pasting notes can be appropriate and eliminate the need to create every part of a note and re-interview patients about their medical histories.

• HHS-OIG identifies “illegitimate use of cut-and-paste record cloning” as a problem.

• Defaulting or copying and pasting clinical information with previous existing documentation from other patient encounters in a different health record facilitates billing at a higher level of service than was actually provided.
Cloning

• Copying and pasting previously recorded information from a prior note into a new note

• The medical record must contain documentation showing the differences and the needs of the patient for each visit or encounter.

• Simply changing the date on the EHR without reflecting what occurred during the actual visit is not acceptable.

• Office of Inspector General (HHS-OIG) 2013 Workplan indicated that due to the growing problem of cloning, its staff would be paying close attention to EHR cloning.
Definitions

• Automated Change of Note Author
  • Automatically changing authorship of a note written by someone else to the current user of the note

• Templates
  • Using predefined text and text options to document the patient visit within a note

• Macros
  • Expanding text associated with abbreviations or specific keystrokes

• Populating via Default
  • Generating content without positive action or selection by author
Author Identification

• “Abuse” describes incidents or practices that may not be fraudulent
  • Not consistent with accepted medical or business practices or may result in unnecessary costs.

• Some incidents directly relate to EHR software features
  • Allowing multiple providers to add text to the same progress note but not allowing each provider to sign, making it impossible to verify the actual service provider or the amount of work performed by each provider.
Templates, Macros, and Population via Default

Templates that complete forms by checking a box

Macros that fill in information by typing a key word

Auto-population of text when it is not entered
Templates, Macros, and Population via Default

• **Issues**

  • Structure of the note is not a good clinical fit
    • Does not accurately reflect the patient’s condition and services
  
  • Features may encourage over-documentation to meet reimbursement requirements even when services are not medically necessary or are never delivered.
Definitions

• Audit Trail
  • Tracking EHR access information, including the username, workstation, and document event description (for example, amendment, correction, or deletion), and date and time

• Fabrication
  • Copying information or creating text to show that treatment was delivered or occurred at a higher level.
Standards & Policies

• Standards of conduct should convey the expectation that employees will act in an appropriate and lawful manner

  • Failure to do so could result in termination.

• Policies should make clear who can have access to EHRs and when, and which system features (for example, copy and paste, auto-population) can be used in which sections of a record.

• CMS requires that EHRs provided to program integrity contractors clearly identify any amendment and “provide a reliable means to clearly identify the original content, the modified content, and the date and authorship of each modification of the record.”
Program Integrity Vulnerabilities

- EHR Technology gives easy access to sort, retrieve and export a large amount of data quickly

- CASE:
  - ER employee viewed records
    - Identified those in traffic accidents
    - Relayed contact and injury information
Provider Education

• Provider education helps correct vulnerabilities
  • Maintain proper documentation
  • Reduce inappropriate claims submission
  • Protect patient and provider identity information
  • Establish a broader culture of compliance
Sample Compliance Checklists for Electronic Health Records
Development

• Implementation of electronic health records (EHRs) requires selecting the appropriate software
  • Following applicable Federal and State privacy and security regulations and guidance.

• Providers and others should develop
  • Management tools
  • Standards and policies
    • To strengthen business operations and provide guidance to staff to protect the security and integrity of EHRs
Compliance Program

• A condition of enrollment in Medicare and Medicaid providers are required to have a compliance program containing core elements for providers or suppliers within a particular industry or category

• Required by Affordable Care Act
Standards of Conduct

• Information about the medical conditions, medical history, medications, and treatment of patients is sensitive information protected by privacy and security laws.

• Each employee is responsible for keeping this information confidential, private, and secure.
## Sample Checklist 1. Standards of Conduct

<table>
<thead>
<tr>
<th>Do the Standards of Conduct address employee responsibility for: [7, 8, 9, 10]</th>
<th>Yes or No</th>
</tr>
</thead>
</table>

### Area: Integrity

| The appropriate use of EHRs? | □ Yes □ No |
| The accuracy and integrity of information in the patient’s EHR? | □ Yes □ No |
| Acting in an ethical and lawful manner? | □ Yes □ No |
| Protecting the integrity of the EHR? | □ Yes □ No |

### Area: Security

| Appropriate EHR system access? | □ Yes □ No |
| Keeping confidential and private health information safe? | □ Yes □ No |
| Ensuring that confidential information is securely stored and appropriately disposed of according to Federal and State requirements where applicable? | □ Yes □ No |
| Reporting suspected problems, such as security breaches, unauthorized access, or other suspicious activity? | □ Yes □ No |
Policies & Procedures

• Use following checklist when creating or updating policies and procedures to ensure EHR-related program integrity vulnerabilities are addressed

• Place a check next to each EHR feature or action if it is included in the existing policies and procedures

• Leave the field blank if the feature or action is not included

• Consider revising policies and procedures to include any missing EHR features or actions
## Sample Checklist 2. Policies and Procedures

<table>
<thead>
<tr>
<th>Do the policies and procedures address:</th>
<th>Check for Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. How to use EHR system security features, including:</strong> [12, 13, 14]</td>
<td></td>
</tr>
<tr>
<td><strong>Audit log:</strong> Keep the audit log enabled at all times so it creates an accurate chronological history of changes to EHR. Procedures should describe exceptions, such as who can disable the log and under what circumstances.</td>
<td></td>
</tr>
<tr>
<td><strong>Access restrictions:</strong> Identify levels of access for user groups; address password sharing and logging in to multiple computers at the same time; identify who sets access restrictions and under what circumstances they can change them.</td>
<td></td>
</tr>
<tr>
<td><strong>Alerts and warnings (for example, drug interactions):</strong> Identify whether it is appropriate to disable and when.</td>
<td></td>
</tr>
<tr>
<td><strong>Templates:</strong> Address when to use templates and whether to supplement with free text.</td>
<td></td>
</tr>
<tr>
<td><strong>Macros:</strong> Address when to use macros, whether to supplement with free text, and where and how to use them.</td>
<td></td>
</tr>
<tr>
<td><strong>Auto-population via default:</strong> Address whether to use this feature, whether to supplement it with free text, and where and how to use it.</td>
<td></td>
</tr>
</tbody>
</table>
2. How to appropriately use EHR system documentation features and capabilities, including:[15]

| Feature Description                                                                 | YES
|--------------------------------------------------------------------------------------|----
| Auto-population via checkbox: Address whether to use this feature, whether to supplement it with free text, and where and how to use it. | Yes
| Authorization of documentation (for example, date, time, original author, amendments, corrections, reasons for change): Address what circumstances justify making changes to the EHR; identify who can make changes; identify requirements for amendments and corrections to an EHR; and identify what information cannot be changed (author, date, and time of original note). | Yes
| Automated change of note author: Identify the circumstances that allows enabling or disabling this feature and who has authority to do it. | Yes
| Copy and paste or cloning: Address whether using this capability is acceptable and under what circumstances, whether it must be identified as copied text, and if it must be supplemented with free text. | Yes
| Copy forward: Address whether use is acceptable and under what circumstances, whether it must be identified as copied text, and if it must be supplemented with free text. | Yes
| Cut and Paste: Address why not to allow this. | Yes
3. How to prevent intentional deception or misrepresentation that results in an unauthorized benefit: [16]

<table>
<thead>
<tr>
<th>Statement</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a statement that all violations of policy are subject to disciplinary action.</td>
<td>☐</td>
</tr>
<tr>
<td>Include a statement that prohibits over-documentation to improve reimbursement.</td>
<td>☐</td>
</tr>
<tr>
<td>Include a statement that prohibits fabrication of records to receive reimbursement.</td>
<td>☐</td>
</tr>
<tr>
<td>Include a statement that prohibits false attribution of work performed by others.</td>
<td>☐</td>
</tr>
</tbody>
</table>
4. How to detect, correct, and report potential fraud, waste, abuse, and improper payments, including:[17]

<table>
<thead>
<tr>
<th><strong>Internal monitoring:</strong> Identify who is responsible, and address how and how often to do it, how to identify areas and elements, and how to share results.</th>
<th>☐ Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Periodic auditing:</strong> Identify who is responsible, and address how often to do it, how to identify areas and elements, and how to share results.</td>
<td>☐ Yes</td>
</tr>
<tr>
<td><strong>Use of disciplinary actions:</strong> Identify what disciplinary actions may be taken and how and when to implement them, and identify a process for evaluation.</td>
<td>☐ Yes</td>
</tr>
<tr>
<td><strong>Corrective actions:</strong> Identify what corrective actions may include and how to implement them. Identify a process for evaluation of action taken.</td>
<td>☐ Yes</td>
</tr>
<tr>
<td><strong>Investigating and reporting suspected fraudulent activities:</strong> Identify how to report fraudulent activities; who is responsible for investigation; and when to refer activities to law enforcement.</td>
<td>☐ Yes</td>
</tr>
</tbody>
</table>
5. **How program integrity policies and procedures should be included in staff and management training, including:** [18]

<table>
<thead>
<tr>
<th>Category</th>
<th>Yes/No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriate use of EHR features and capabilities.</td>
<td>Yes</td>
</tr>
<tr>
<td>Protection of the integrity of documentation.</td>
<td>Yes</td>
</tr>
<tr>
<td>Protocols for reporting suspected fraud, waste, and abuse.</td>
<td>Yes</td>
</tr>
<tr>
<td>Disciplinary actions.</td>
<td>Yes</td>
</tr>
<tr>
<td>Prevention of fraud, waste, abuse, and improper payments.</td>
<td>Yes</td>
</tr>
<tr>
<td>Standards of conduct and policies.</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Preparing & Responding to Audits of Electronic Health Records

• Regulatory agencies or integrity contractors audit
  • Part of regular compliance problem
  • Random or deliberate selection
• Providers should perform periodic internal and external audits
  • Measure, correct and prevent improper payments
  • Strengthen integrity of claims and payment process
Preparing & Responding to Audits of Electronic Health Records

- Checklist helps to prepare for an electronic health record (EHR) system internal or external audit
  - Addresses how to respond to auditors during audit
  - Addresses how to follow up after the audit
- Items on the checklist should be typical components of internal training to prevent
  - Fraud
  - Waste
  - Abuse
### Sample Checklist 1. Provider Audit Preparation

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

---

**HEALTHCON**  

---

**AAPC**
## Sample Checklist 2. Addressing Audit Findings

<table>
<thead>
<tr>
<th>Actions to be taken by the audit response team</th>
<th>Check for Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the contents of the final audit report and discuss the findings.</td>
<td>□ Yes</td>
</tr>
<tr>
<td>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).</td>
<td>□ Yes</td>
</tr>
<tr>
<td>Designate staff responsible for developing a corrective action plan to address each of the comments and findings.</td>
<td>□ Yes</td>
</tr>
<tr>
<td>Review and implement the corrective action plans that address each comment or finding.</td>
<td>□ Yes</td>
</tr>
<tr>
<td>Set dates for completing each item.</td>
<td>□ Yes</td>
</tr>
<tr>
<td>Establish a plan to monitor and audit to determine the effectiveness of the changes.</td>
<td>□ Yes</td>
</tr>
</tbody>
</table>
Conducting Internal Monitoring & Auditing

- Compliance program should include
  - Internal & external auditing
- Monitoring is an ongoing effort
  - To ensure that policies and procedures are in place
    - Are being followed
  - Should take place on a regular basis during normal operations
Conducting Internal Monitoring

- Identify risks
- Do a baseline audit
- Develop and implement a plan for ongoing monitoring
- Perform corrective action
Conducting Internal Audit

• Internal audit different from monitoring
  • Done periodically (not ongoing)
  • More focused
  • More comprehensive
  • Based on specific pre-determined standards
  • Determine compliance with standards
  • Should occur at least once a year
  • Those conducting audit should be different than those who conduct monitoring
Conducting Internal Audit

- Identify Risks
- Audit the Risks
- Document the audit
- Review and act on the audit results
Figure 1. Relationship Between Monitoring and Auditing
Corrective Action

- Returning funds
- Disciplinary action
- Changing or updating computer software & systems
- Revising policies
Corrective Action

- Employee training
  - Possible re-training
- Refer criminal violations to appropriate agency for further investigation
Conclusion

• Properly implemented and supported EHR systems can:
  • Improve quality and coordination of care
  • Reduce costs
  • Better preserve information from natural or manmade disasters
  • Better protect patient privacy
  • Reduce the incidence of fraud
TO OBTAIN BENEFITS

• Providers must
  • Incorporate and use fraud prevention features in their EHR software
  • Adopt appropriate policies that mitigate the risks of improper use
QUESTIONS???

Thank you!

Jill@youngmedconsult.com