Sample Compliance Checklists for Electronic Health Records

Introduction

The implementation of electronic health records (EHRs) requires selecting the appropriate software and following applicable Federal and State privacy and security regulations and guidance. Additionally, providers and others should develop management tools, including standards and policies, to strengthen business operations and provide guidance to staff to protect the security and integrity of EHRs. A compliance program is voluntary for various providers and suppliers;[1] however, the Affordable Care Act[2, 3] requires the Secretary of the U.S. Department of Health and Human Services (HHS) to establish, as a condition of enrollment in Medicare and Medicaid, a compliance program containing core elements for providers or suppliers within a particular industry or category.[4]

Both the Standards of Conduct and Policies and Procedures checklists within this document include areas that providers should address to protect the integrity and security of EHR data. The extent to which a provider addresses these areas may differ depending on the size of the practice or organization.

Standards of Conduct

Standards of conduct convey the practice's operating principles and values. They should include the expectation that all employees conduct themselves in an ethical, compliant, and lawful manner.[5, 6] An example of an element that is typically part of a standards of conduct document is listed before the table. Sample Checklist 1. Standards of Conduct describes EHR integrity and security areas related to EHRs. The checklist recommends elements that should be included in the standards of conduct. If the element is included in the current standards of conduct, check the "Yes" box. If the element is missing from the standards of conduct, check the "No" box and revise the standards to include the missing element.

Example

Standard of Conduct: Information about the medical conditions, medical history, medications, and treatment of our 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

Do the Standards of Conduct address employee responsibility for:[7, 8, 9, 10]	**Yes or No**
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 and Procedures

Policies and procedures provide the framework for meeting compliance.[11] Providers and others should review their current policies and procedures to ensure that they address current compliance issues. If no policies and procedures exist, providers should create them. An example of a policy and procedure for consideration follows.

Example

Policy: It is Family Medical Group's policy for all employees and associates to attend mandatory compliance training within 30 days of hire and annually thereafter. The mandatory training includes specialized compliance training on the appropriate use of

the EHR system features and capabilities and data security during daily use, transition, storage, and disposal.

Corresponding Procedure: Family Medical Group office manager and owners will:

- Develop the training based on practice policy;
- Ensure training is delivered in the appropriate format within the required time frames;
- Ensure all employees and owners complete the training and achieve the required level of competency; and
- Take appropriate action should an employee not meet the training requirements.

Policies and Procedures for Electronic Health Record Use

Use Sample Checklist 2. Policies and Procedures 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. Providers should consider revising policies and procedures to include any missing EHR features or actions.

Sample Checklist 2. Policies and Procedures

Do the policies and procedures address:	Check for Yes
1. How to use EHR system security features, including:[12, 13, 14]	
Audit log: 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.	☐ Yes
Access restrictions: 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.	☐ Yes
Alerts and warnings (for example, drug interactions): Identify whether it is appropriate to disable and when.	☐ Yes

2. How to appropriately use EHR system documentation features and capabilities, including:[15]	
Templates: Address when to use templates and whether to supplement with free text.	☐ Yes
Macros: Address when to use macros, whether to supplement with free text, and where and how to use them.	☐ Yes
Auto-population via default: Address whether to use this feature, whether to supplement it with free text, and where and how to use it.	☐ 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]	
Include a statement that all violations of policy are subject to disciplinary action.	☐ Yes
Include a statement that prohibits overdocumentation to improve reimbursement.	☐ Yes

Include a statement that prohibits fabrication of records to receive reimbursement.	☐ Yes
Include a statement that prohibits false attribution of work performed by others.	☐ Yes
4. How to detect, correct, and report potential fraud, waste, abuse, and improper payments, including:[17]	
Internal monitoring: Identify who is responsible, and address how and how often to do it, how to identify areas and elements, and how to share results.	☐ Yes
Periodic auditing: Identify who is responsible, and address how often to do it, how to identify areas and elements, and how to share results.	☐ Yes
Use of disciplinary actions: Identify what disciplinary actions may be taken and how and when to implement them, and identify a process for evaluation.	☐ Yes
Corrective actions: Identify what corrective actions may include and how to implement them. Identify a process for evaluation of action taken.	☐ Yes
Investigating and reporting suspected fraudulent activities: Identify how to report fraudulent activities; who is responsible for investigation; and when to refer activities to law enforcement.	☐ Yes
5. How program integrity policies and procedures should be included in staff and management training, including:[18]	
Appropriate use of EHR features and capabilities.	☐ Yes
Protection of the integrity of documentation.	☐ Yes
Protocols for reporting suspected fraud, waste, and abuse.	☐ Yes
Disciplinary actions.	☐ Yes
Prevention of fraud, waste, abuse, and improper payments.	☐ Yes
Standards of conduct and policies.	☐ Yes

Additional Resources

Many policy and procedure templates are available on the Internet to assist with language and format. For example, a security policy template is posted to https://www.healthit.gov/providers-professionals/implementation-resources/information-security-policy-templat on the HealthIT website.

To see the electronic version of this checklist 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

References

1 U.S. Department of Health and Human Services. Office of Inspector General. Compliance Guidance. Retrieved April 8, 2016, from https://oig.hhs.gov/compliance/compliance-guidance

2 Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6401(b)(1), 124 Stat. 119, 752. (2010, March 23). Retrieved April 8, 2016, from http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf

3 Health Care and Education Reconciliation Act, Pub. L. No. 111-152, 124 Stat. 1029. (2010, March 30). Retrieved April 8, 2016, from http://www.gpo.gov/fdsys/pkg/PLAW-111publ152/pdf/PLAW-111publ152.pdf

4 Social Security Act § 1902(kk)(5). Retrieved April 8, 2016, from http://www.ssa.gov/OP_Home/ssact/title19/1902.htm

5 Centers for Medicare & Medicaid Services. (2013, January 11). Medicare Managed Care Manual. Chapter 21, Section 50.1.1. Retrieved April 8, 2016, from http://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf

6 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. Retrieved April 8, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

7 American Health Information Management Association. (2013). Integrity of the Healthcare Record: Best Practices for EHR documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

8 American Health Information Management Association. (2011, October 2). AHIMA Code of Ethics, §§ 3.1, 4.1, 4.8. Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=105098

9 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule. 45 C.F.R. § 170.315(d)(1). Retrieved April 8, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

10 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. 59443. Retrieved April 8, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

11 U.S. Department of Health and Human Services. (2007, March). HIPAA Security Series 5. Security Standards: Organizational, Policies and Procedures and Documentation Requirements. Retrieved April 8, 2016, from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/pprequirements.pdf

12 U.S. Department of Health and Human Services. (2015, October 16). 2015 Edition Health Information Technology (Health IT) Certification Criteria, 2015 Edition Base Electronic Health Record (EHR) Definition, and ONC Health IT Certification Program Modifications; Final Rule. 45 C.F.R. § 170.315(d)(2). Retrieved April 8, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2015-10-16/pdf/2015-25597.pdf

13 U.S. Department of Health and Human Services. Office of the Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (pp. 9, 11). Retrieved April 8, 2016, from https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

14 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

15 American Health Information Management Association. (2013, August). Integrity of the Healthcare Record: Best Practices for EHR Documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

16 Association of American Medical Colleges. AAMC Compliance Officers' Forum. (2011, July 11). Electronic Health Records in Academic Medical Centers Compliance Advisory 2. Retrieved June 12, 2015, from https://www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf

17 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. 59443. Retrieved June 12, 2015, from http://oig.hhs.gov/authorities/docs/physician.pdf

18 American Health Information Management Association. (2013). Integrity of the Healthcare Record: Best Practices for EHR documentation (2013 Update). Retrieved April 14, 2016, from http://library.ahima.org/doc?oid=300257

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