Fact Sheet

A Compliance Program for Electronic Health Records

Introduction

With the increasing use of electronic health records (EHRs), providers need to adapt to and change how they identify and address program integrity vulnerabilities. Providers and others can address this need by developing management tools to strengthen business operations and by providing guidance to staff as part of the EHR implementation process.

Compliance Program Guidance

The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) issued general health care compliance program guidance that includes seven components to help providers and suppliers develop an effective compliance program.[1] The components include designating a compliance officer, effective communication, written policies and procedures and standards of conduct, appropriate staff education and training, enforcing disciplinary standards, internal monitoring, and promptly responding to detected offenses through appropriate corrective action.[2] While implementing a compliance program is voluntary for various providers and suppliers,[3] the Affordable Care Act[4] requires the Secretary of 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.[5]

Although the HHS-OIG guidance is voluntary, they strongly suggest the seven components are an effective way to reduce fraud, waste, and abuse. Providers and others should follow this guidance to take preventive action to deter inappropriate use of EHR system features or access to patient information.[6] Developing internal controls through a compliance program will help streamline the workflow and prevent and reduce improper conduct.[7]

Policies and Procedures and Standards of Conduct

Providers can take steps to prevent program integrity risks by adopting policies and procedures and standards of conduct for proper EHR use. Policies and procedures provide the framework for meeting compliance.[8] Providers should review their current policies and procedures to ensure they address compliance issues. If no policies and procedures exist, providers and others should create them. Free templates are available online that will help with language and format.

Written policies and procedures should include items relevant to the implementation and daily use of EHRs. Policies and procedures related to health information management should clearly identify security measures that staff should follow to control access and to ensure the protection of data in transit, in storage, or awaiting disposal from theft or alteration.[9] Additionally, policies and procedures should address clinical and administrative documentation requirements such as copying and pasting; disabling system features; and how to use templates, macros, and auto-population via default.[10] Policies and procedures should provide instruction for reporting potential fraud, waste, and abuse; clearly state disciplinary action; and make training a requirement for all staff.[11] In addition, always check the latest Federal rules and regulations to keep up to date with any new requirements.

Standards of conduct convey the principles and values of the practice and should include the expectation that all employees conduct themselves in an ethical, compliant, and lawful manner.[12, 13] Standards of conduct would include the ongoing expectation that employees follow Federal and State statutes, regulations, and guidance for data security, as well as internal policies and procedures for EHR use.

Tools to assist in creating or updating standards of conduct and policies and procedures are available in the "Compliance Checklist for Electronic Health Records" posted to https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/electronic-health-records.html on the Centers for Medicare & Medicaid Services (CMS) website.

Education and Training

Education and training are important components of a compliance program. These components ensure employees are aware of the policies, procedures, and other job requirements and that compliance with these requirements is a condition of employment.[14] One initiative found that training on the features of an area-wide

e-prescribing system and capabilities is more effective when provided by internal management rather than a vendor, and includes the appropriate use of the technology according to the established policies and procedures.[15] Effective practices for a training program include annual training and supporting documentation specifying the date and time of training as well as attendees.[16]

Ongoing prevention education for staff should include sharing results of monitoring reports.[17] Monitoring reports can provide examples of inappropriate access or legitimate actions identified as suspicious.

Conclusion

A compliance program can provide the foundation for cohesive workflow and reduce the potential risks for fraud, waste, abuse, and improper payments. The implementation of a compliance program is voluntary. However, providers and others can prevent risks in the transition to and daily use of EHRs through an effective compliance program.

To see the electronic version of this fact sheet 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.

References

1 U.S. Department of Health and Human Services. Office of Inspector General. Compliance Guidance. Retrieved April 4, 2016, from http://oig.hhs.gov/compliance/compliance-guidance

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. Retrieved April 4, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

3 U.S. Department of Health and Human Services. Office of Inspector General. Compliance Guidance. Retrieved April 4, 2016, from http://oig.hhs.gov/compliance/compliance-guidance

4 Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6401(b)(1), 124 Stat. 119, 751. (2010, March 23). Retrieved April 4, 2016, from http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/pdf/PLAW-111publ148.pdf

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

6 U.S. Department of Health and Human Services. Office of Inspector General. (2013, December). Not All Recommended Fraud Safeguards Have Been Implemented in Hospital EHR Technology (pp. 9, 11). Retrieved April 4, 2016, from https://oig.hhs.gov/oei/reports/oei-01-11-00570.pdf

7 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 4, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

8 U.S. Department of Health and Human Services. Office of Inspector General. (2015, April 20). Practical Guidance for Health Care Governing Boards on Compliance Oversight. Retrieved April 4, 2016, from http://oig.hhs.gov/compliance/compliance-guidance/docs/Practical-Guidance-for-Health-Care-Boards-on-Compliance-Oversight.pdf

9 Kim, J., Grillo, J., Boxwala, A., Jiang, X., Mandelbaum, R., Patel, B., Ohno-Machado, L. (2011, October 22). Anomaly and Signature Filtering Improve Classifier Performance for Detection of Suspicious Access to EHRs (p. 723). American Medical Informatics Association Annual Symposium Proceedings Archive 2011; 2011: 723–731. Retrieved April 4, 2016, from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3243249/

10 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

11 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 4, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

12 Centers for Medicare & Medicaid Services. (2013, January 11). Medicare Managed Care Manual. Chapter 21, Section 50.1.1. Retrieved April 4, 2016, from https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf

13 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 4, 2016, from http://oig.hhs.gov/authorities/docs/physician.pdf

14 Centers for Medicare & Medicaid Services. (2013, January 11). Medicare Managed Care Manual. Chapter 21, Section 50.3. Retrieved April 5, 2016, from https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/mc86c21.pdf

15 Point-of-Care Partners. (2013, April). Building the Foundation for an Effective and Efficient Healthcare System: Lessons Learned in Southeastern Michigan. Retrieved April 5, 2016, from http://www.pocp.com/publications/semi-hit-lessons-learned-wp.pdf

16 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

17 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 fact sheet 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 fact sheet was prepared as a service to the public and is not intended to grant rights or impose obligations. This fact sheet 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