COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Health Information Management: Electronic Health Record Systems

By K. Mark Jenkins,[1] CPA (TN), CHC, CHPC, CHRC, CIA, CFE, CGMA, CHCO

What Are Electronic Health Record Systems?

Prior to electronic health records (EHR), all medical records were kept as paper copies in manual filing systems with each clinician's (doctor, nurse practitioner, etc.) office and hospital, clinic, or surgery center utilized by a patient over the course of their lives. From the healthiest individuals who only sought episodic care to treat things such as ear infections and the flu to the sickest individuals with multiple illnesses and comorbid conditions, their medical histories (care notes, lab results, medications, etc.) were all written and maintained on paper in various locations.

In the mid-1960s, various technology and engineering companies began developing EHR systems. This was not an overnight one-stop shop for medical records. Many independent systems were developed for medical specialty areas these systems ultimately improved care and documentation, but they were each independent systems. These standalone systems (called "subsystems") were in many cases connected to a core medical record system. In many large healthcare systems, this has meant that up to 400 independent subsystems were linked to form a consolidated view of a patient's medical record. In many cases, the billing component of healthcare services was not integrated into the EHR system until long after the systems were created, resulting in unique compliance challenges for compliant records and billing.

As EHRs advanced and funding increased to implement these systems, the field of EHR system developers reduced and consolidated, and today a few more fully integrated systems are primarily utilized by healthcare organizations. Although these systems all have primary functionality (which house patient encounters and episodes of care, orders, lab tests, radiological images, billing and collection records, etc.), all have also been implemented uniquely by different healthcare organizations. The core systems—as well as the implemented customizations at each entity—increase compliance and other risks, which must be mitigated.

Often EHR system implementation involves building the new system to do things as the organization did them in the past (either through paper documentation or older EHR systems), which can create or even further compliance issues and concerns. There are also features built within each EHR core system—which were developed by well-meaning engineers with clinician input—that can be manipulated by in-house system designers. These features are intended to increase productivity and reduce documentation and other burdens, but they cause increased documentation risks.

EHR systems have revolutionized healthcare in many ways: theoretically providing real-time access to complete medical records and history to healthcare providers and patients; increasing the capability to diagnose diseases, reduce medical errors, and improve outcomes; allowing multiple clinicians access to medical record information at the same time; and many other ways.

Most EHR systems allow for a wide variety of implementation, from out-of-the-box (standard) implementation to customized implementation. Compliance needs to be involved in decisions about a healthcare organization's EHR system from the start. Even out-of-the-box implementations can have features that do not align with good

internal controls and processes. The higher the customization, the higher the compliance risk. With a fully integrated EHR system—where one system has clinician documentation (for clinic and inpatient services), billing module(s), subsystems such as radiology, etc.—there are increased opportunities for a single change in the system to help or fix one situation that may impact downstream processes or outputs. Therefore, it is critical that compliance professionals be included in development, deployment, and ongoing changes with EHR systems.

EHR systems promise capabilities to streamline documentation; however, most clinicians find documentation in these systems to be extremely labor and time extensive. This has caused the development of many tools and templates, which tends to increase compliance risks and the need for compliance's involvement both at the beginning of an EHR implementation and when templates and other tools are updated. The goal to reduce the number of "clicks" a clinician must make to develop their documentation has often led to standardized "template" language and use of phrases and links (tools generally part of the EHR package) to write the note. While these tools have their advantages, they increase compliance risks. In many cases, documentation appears the same visit after visit with clinicians not making impactful changes/updates to the documentation for the patient interaction. While each organization must determine their risk tolerance for documentation clarity, we all want each patient encounter/interaction to be uniquely documented in the medical record to help ensure continuity of care and patient safety.

Risk Area Governance

Joint Commission and the Centers for Medicare & Medicaid Services

Both have medical record signature requirements that extend to paper and electronic signatures. EHRs must have the ability to track various forms of authentication (of orders, reviews, documentation, etc.). The signature must include the date and time.

Health Information Technology for Economic and Clinical Health (HITECH) Act,42 U.S.C. § 1395w-4(o)(2)

This act provides the U.S. Department of Health and Human Services with the authority to establish programs to improve healthcare quality, safety, and efficiency through the promotion of health IT, including EHRs and private and secure electronic health information exchange. EHRs must comply with various provisions of the HITECH Act. The act also increased penalties for violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.[2]

Many rules govern documentation standards for medical records to support billing for medical services. These include the following: False Claims Act (FCA), HIPAA, Joint Commission and the Centers for Medicare & Medicaid Services (CMS), and 42 C.F.R. § 482.24, Condition of participation: Medical record services.

False Claims Act, 31 U.S.C. §§ 3729-3733

The FCA makes it a crime for any person or organization to knowingly make a false record or file a false claim regarding any healthcare program funded directly by the United States government or any state healthcare system. There has been a significant increase in FCA cases regarding allegations of false claims to Medicare and Medicaid, pursuant to the Electronic Health Records Incentive Program. In addition, the FCA has also been triggered related to fraudulent arrangements tied to implementation and use of EHRs. Inappropriately configured EHRs can cause false claims to be submitted due to documentation inconsistencies or inaccuracies.[3]

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat.

1936

HIPAA rules relate to privacy, security, and EHRs. EHRs must have appropriate controls to protect the data internally and externally. It is imperative that health systems have access controls, encryption, and the ability to track all access to records.[4]

CMS Condition of Participation: Medical Record Services, 42 C.F.R. § 482.24

This rule requires hospitals to have administrative responsibilities for medical records and that a medical record must be maintained for every individual evaluated or treated.[5]