COMPLIANCE IN THE AGE OF ELECTRONIC MEDICAL RECORDS

Ranjan Sachdev, M.D.
Abby Pendleton, Esq.
Jessica L. Gustafson, Esq.

Health care providers are facing unprecedented scrutiny in the submission of claims. For example, with respect to Medicare claims, not only do Medicare Affiliated Contractors ("MACs") (or Medicare Carriers and Intermediaries) conduct their own audits, but also Medicare's Recovery Audit Contractor ("RAC") program is now operational nationwide (and is expanding to include Part C and Part D claims), and Zone Program Integrity Auditors ("ZPICs") (or Program Safeguard Contractors ("PSCs")) are conducting nationwide benefit integrity audits. With respect to Medicaid claims, Medicaid Integrity Contractors ("MICs") are actively auditing claims, and the RAC program is expanding to include Medicaid claims as well. Health care providers must be cognizant of this increased claims scrutiny and conduct themselves with an increased focus on compliance. Although using electronic medical records is encouraged by Medicare, Medicaid and other third party payors as a mechanism to improve clinical documentation and by extension to ultimately improve the quality of patient care, certain compliance issues can be heightened with the use of electronic medical records. This article will focus on some of the compliance issues raised by using electronic medical records.

Documentation is key to establish that a service is medically necessary and appropriately coded

Auditors and medical reviewers routinely deny claims because an item or service is found not to be medically necessary, or is found to be inappropriately coded. It is essential that when a health care provider documents a service performed, such documentation must establish for the reviewer the medical necessity for the service rendered and establish that the appropriate code was chosen for the service at issue. Documentation must be thorough. According to the Office of Inspector General ("OIG") Compliance Program for Individual and Small Group Physician Practices, "[O]ne of the most important physician practice compliance issues is appropriate documentation of diagnosis and treatment. Physician documentation is necessary to determine the appropriate medical treatment for the patient and is the basis for coding and billing determinations." 65 Fed. Reg. 59434, 59440 (October 5, 2000).

Keeping in mind that auditors oftentimes are nurse reviewers without specific expertise in a provider's specific practice area, it is essential that documentation paint a picture for a reviewer of medical necessity and appropriate coding, keeping in mind compliance issues specific to electronic medical records that may arise. Each note should establish the medical necessity for the service provided, and should meet the following guidelines:

- Be complete and legible;
- Document each patient encounter including: the reason for the visit; relevant portions of the patient's medical history; physical exam findings; diagnostic test results, if any; assessment; clinical impression/diagnosis; plan of care; date and legible identity of provider;

- Provide the rationale for ordering diagnostic tests and other ancillary services (or it should be easily inferred);
- Support the CPT and ICD-9 codes billed;
- Identify risk factors; and
- Document the patient's progress, his or her response to, and any changes in, treatment, and any revision in diagnosis is documented.

See generally, OIG Compliance Program for Individual and Small Group Physician Practices, 65 Fed. Reg. at 59440.

Compliance issues arising through the use of electronic medical records

1. *Signature Issues*

Medical records must include a legible identifier of the treating provider. Medicare guidelines permit health care providers to sign medical records electronically. Even if a medical record is signed electronically, Medicare guidelines must be satisfied. For example, an electronic signature may not merely be comprised of the typed name of the provider that performed the service at issue, as this does not meet Medicare criteria. An acceptable signature could include a legible full signature, a legible first initial with last name, or an illegible signature over a typed or printed name. *See generally,* Medicare Program Integrity Manual, Chapter 3, Section 3.3.2.4.

The Medicare Program Integrity Manual ("PIM"), Chapter 3, Section 3.3.2.4 sets forth Medicare's signature requirements, and the PIM, Chapter 3, Section 3.3.2.4 E sets forth Medicare's guidelines related to electronic signatures in particular. This portion of the PIM notes that:

> Providers using electronic systems need to recognize that there is a potential for misuse or abuse with alternate signature methods. For example, providers need a system and software products that are protected against modification, etc., and should apply adequate administrative procedures that correspond to recognized standards and laws. The individual whose name is on the alternate signature method and the provider bear the responsibility for the authenticity of the information for which an attestation has been provided. Physicians are encouraged to check with their attorneys and malpractice insurers concerning the use of alternative signature methods.

2. *Issues with self-populating fields, "exploding" documentation*

Most electronic medical records have built in "time savers," such as self populating fields that insert a patient's past medical history into each record by simply selecting a check box. This is sometimes referred to as "exploding" documentation, because information is populated forward with just a click of the mouse. These time saving devices ultimately may hurt the provider if not used correctly. Potential issues with "exploding" documentation could include the following:

- In some cases, not only is a patient's past medical history carried forward by selecting a check box, but also some electronic medical records populate an entire patient assessment just by selecting a check box (*i.e.,* in the case of an evaluation and management ("E/M") service, these types of electronic medical records may populate an entire review of systems). Especially in scenarios where the review of systems does not change from visit note to visit note, or where the review of systems does not appear to be related to the patient's chief complaint, or where the review of systems mistakenly includes information not relevant to the gender of the patient, an auditor may question the integrity of the review of systems and/or may question whether a review took place at all. In these cases, the popular adage, "if it isn't documented, it hasn't been done" does not apply; rather auditors are increasingly taking the position that "if it is documented, then *maybe* it has been done depending on other circumstances." Providers need to be mindful of this reality and ensure that each visit note is tailored to the visit performed. In all cases, only services actually rendered on the particular visit should be documented.

- In some cases, electronic medical records include not only "exploding" documentation, but also include a narrative portion of the record where the provider inserts information specific to his or her patient observations on a given visit. In some cases, this may lead to internally inconsistent documentation. For example, if the electronic medical record defaults to include a statement such as, "Patient presents without pain," but then the narrative portion of the record states "Pt c/o severe pain," an auditor may deny payment with respect to that service because of the inconsistent documentation. Providers must review all information that automatically populates to ensure its accuracy and to make certain the record remains internally consistent. Above all, records must accurately describe the patient's condition and services provided.

- In some cases, electronic medical records systems have been set up to populate information not only prospectively, but also retrospectively, which creates significant risk for the provider. For example, in one recent case, a Medicare Program Safeguard Contractor ("PSC") conducted an audit of a provider with a newly adopted electronic medical record. The provider did not realize that each time diagnostic test results were entered, this information populated into the record prospectively as well as retrospectively. That is, results from a test that took place in February 2010 were included not only in subsequent notes but also were included in notes dating before the test as well (*e.g.*, the results were included in notes from January 2010, December 2009, etc. – all prior to the test). As a result of the audit, the PSC denied payment for all services reviewed, questioning the integrity of all medical records generated by the provider. Instead of acknowledging this issue as a mere technical glitch, the PSC denied payment for all claims reviewed, forcing the provider to resolve the issue through the Medicare appeals process. In many cases, these technical glitches can be addressed in the set up of the electronic medical record system at the time of its adoption.

3. *Issues with electronic medical record templates generally*

In some cases, the electronic medical record template is not sufficiently customized to the provider's specific health care specialty area. In these cases, it may be that the template includes

information that would rarely be relevant to the particular provider (*e.g.,* inclusion of a review of the gastro-intestinal system if the provider is a hand surgeon). Oftentimes, this issue can be addressed through the customization of the template as it is adopted. Providers must keep in mind that medical necessity must predominate.

Another compliance risk area includes those cases where the electronic medical record fails to include a place for the provider to insert a narrative relevant to his or her patient observations on a given visit. Medical records that fail to include this option are at great risk to appear identical to each other. When medical records appear identical from one visit to the next, auditors routinely deny claims for the reason that medical necessity cannot be established.

Recommendations

Many of the compliance issues arising through the use of electronic medical records can be avoided through active provider involvement as an electronic medical record is chosen and implemented. The provider should ensure that it selects an electronic medical record with appropriate security mechanisms in place. Templates included as part of the electronic medical record should be customized to include information relevant to the provider's specialty, and every electronic medical record should encourage narrative statements. Once an electronic medical record system is chosen, the health care provider must educate himself or herself regarding the security mechanisms in place, the general capabilities for the software, printing mechanisms, etc. Providers must always review the finalized record to ensure that the information contained therein is accurate. Not only can the improper use of electronic medical records lead to overpayment demands as a result of audit, but also providers need to be mindful of potential False Claims Act exposure.

All health care providers must be cognizant of the increased scrutiny under which claims are reviewed. In the highly-regulated health care environment, providers are well advised to keep compliance activities in the forefront and keep the tips outlined herein in mind when submitting claims. There are special compliance issues that arise with respect to the use of electronic medical records. Providers using electronic medical records must ensure that they understand the capabilities of the software, have knowledge regarding the fields that may self-populate, and tailor each record to each patient's condition at the time of assessment, painting a picture of medical necessity and appropriate coding.