Fraud and the Electronic Medical Record

Daniel M. Avery, MD

The Electronic Medical Record (EMR) is the newest and most up to date approach to the medical record and its attendant problems of coding, billing, storage and access. Several problems have surfaced with the use of the electronic medical record. The most important of these is fraud. There are multiple categories of electronic medical record fraud including physical presence at the time of service, actual time spent with the patient, automatic additions to the medical record, fraudulently increasing charges, diversion of charges, changing attending physicians, increasing charges, non-attending ordering and billing, false entries and orders, unnecessary/incorrect treatment due to scanning errors, message transmittal, recreation of lost data, recurrent use of incorrect data and fraudulent access to records.

The electronic medical record does not require the physical presence of the attending physician to see patients, order tests, bill or sign charts. The EMR may be signed from a remote location, including another state or country. One can "double productivity" by "appearing" to be in one place while in another. There is no way to tell if the attending physician actually saw the patient without interviewing the patient and even then, it may not even be clear since teaching institutions have residents, interns and students. Notes can be created without the presence of the attending. There is no way to look at the EMR and tell if the attending physician was actually present and saw and examined the patient.

Actual time spent with the patient can be obscured by adding information to the current chart that is already in the EMR from previous visits to create a more sophisticated document with a higher charge than from a brief visit. "Up-scaling the charge" is the term applied to increasing the charges by automatic additions to the medical record when only minimal time is spent with the patient. Fraudulently increasing charges can also be achieved by adding laboratory tests, procedures, radiographic studies and injections in any physician's name regardless of which physician, if any, actually saw the patient.

A major area of fraud in the EMR is diversion of charges. Before the EMR chart is completed, closed and signed, anyone with access to the system can enter the chart and change the attending physician of record who actually saw the patient and divert charges to another physician. One physician can see the patient, create a note, code and charge for the visit and sustain the medical liability and responsibility for that visit, yet have the documentation and charge for that visit be diverted to another physician. This problem is often discovered when a patient calls the office and inquires as to why she received a bill from a physician that she did not see.

In large clinics where there are many patients with the same name distinguished only by date of birth and/or social security number, chart entries, diagnoses and orders on the wrong patient can occur very easily. False entries in the EMR then foster the potential for unnecessary, incorrect and inappropriate treatment. Scanning data into the wrong chart promulgates the same set of problems. Message transmittal about the wrong patient or into the wrong chart has the same effect.

Lost data such as patient notes, orders and entries is inherent in computers when the system "goes down." If information is lost immediately, recreation is usually possible. If time has lapsed, it is not. Making up a note is the fraudulent recipe for a disaster. A recreated note for the EMR, a re-dictated, lost or never dictated operative note or history and physical "by wrote" is of no redeeming value. Subsequent treatment based on fabricated data would be at the very best incorrect. It is better to indicate in the chart and to the patient that the patient visit record was lost. Often the patient can at least help create a more accurate history. Most patients understand loss of information from computers. If the note is lost, make a note in the chart and do not charge the patient for the office visit.

With each new patient, referral, consultation and yearly examination, a complete database should be obtained and updated with subsequent visits. Incorrect entries can be ongoing errors with the potential for incorrect or unnecessary treatment based on them if not asked and corrected each patient visit.

Once healthcare providers have access to the EMR and signed privacy and HIPAA agreements, access to medical records is unlimited. Only periodic audits of those entering charts even remotely hint at the opportunity to access a patient's medical records. It is very simple to get a copy of a patient's records, even outside the institution. While viewing the monitor screen, one must only press the print button, completely excluding the medical record department. Physicians, nurses and staff who leave the institution may still access patients' charts and copy records from a remote site if their password into the system is not terminated when they leave. Consider the scenario in which a physician leaves the practice and needs a patient's records. It is very simple to get them through the EMR without anyone knowing about it.

The area of fraud in the EMR still has many challenges ahead. As EMR's become more sophisticated this area must be corrected. The medical liability industry will have to work hand-in-hand with the electronic medical record industry to achieve these goals.