The Changing Face of Healthcare Fraud and Abuse in America

Numa Ray Lee, D.D.S.
Oyster Point Oral and Facial Surgery
Newport News, VA 23606

October 4, 2014

The first False Claims Act was signed into law at the end of the Civil War by President Lincoln, after reports that suppliers to the Union Army sold shoddy or broken war equipment, sickly horses or mules, and rotten food. Fast forward to 2015 and the federal healthcare fraud program has burgeoned into a billion dollar-a-year industry—with the federal government assembling a growing army of attorneys, agents, analysts and auditors on its side. And its attention is riveted on fraud and abuse perpetrated upon the Medicare and Medicaid programs.  

Today’s laws encompass computer billing, coding, the millions of claims submitted, and the multiple locations to which records are sent.

Since enactment of the 1986 False Claims Act (FCA), healthcare fraud and abuse in America has been a hot target for the inspector general. The initial fines under the FCA were $5,500-$11,000 per false claim. In 1993, the attorney general declared that healthcare fraud and abuse would be top priority for the Department of Justice. And in 1995, the Health Insurance Portability and Accountability Act (HIPPA) established the Healthcare Fraud and Abuse Control Program (HCFAC).

---

The HCFAC collected over $11.2 billion in fraudulent claims between 1997 and 2001 increasing to $1.8 billion in 2007 alone.\(^2\) The Office of the Inspector General (OIG) estimates that their efforts have saved the Medicare and Medicaid programs $39 billion.\(^3\)

Fraud is defined as knowingly and willingly executing and/or attempting execution of a scheme … to defraud any healthcare program or to obtain by means of false or fraudulent pretenses, representation, or promises any of the money or property owned by … any healthcare benefit program.\(^4\)

Abuse is defined as acts that are inconsistent with sound medical or business practice without the ability to prove that the act was committed knowingly, willfully and intentionally.\(^5\)

Physicians, nurses, skilled nursing organizations, office workers and suppliers have all been the focus of OIG investigations.

An example of a fraud and abuse case is that of three Indiana dentists charged with Medicaid fraud for allegedly billing Medicaid for services that were not provided; billing for deep sedation when one of the offices lacked the equipment to administer it; and submitting claims in the name of a dentist who no longer worked at the practice. Four office workers were also charged with prescription drug fraud and forgery. The charges were brought by the Indiana Attorney General Greg Zoeller in April, 2014.\(^6\)

Another example is an Augusta, Georgia optometrist whose attorney claimed that the doctor’s fraudulent Medicare billings were merely errors, but who billed for 177, 45-minute

---


\(^3\) Ibid. p. 25

\(^4\) Nelson Bolin, J, etal. Ibid.


comprehensive exams in one day. The optometrist was sentenced January 9, 2014 to 33 months in prison and ordered to pay $441,000 in restitution.⁷

The federal government is spending over $22 billion to encourage hospitals and doctors to adopt Electronic Health Records (EHR) but it has failed to place safeguards to prevent the technology from being used fraudulently, whether deliberately or not.⁸ This means that doctors and office managers must adopt what Ronald Reagan called “trust and verify” techniques.

In a private practice, office staff must be ever vigilant. Beware of coding errors, typos and cut-and-paste billings. A mistake can cost you up to $11,000. And don’t even think about deliberately defrauding the healthcare system. Fines in the tens of thousands of dollars coupled with jail time are commonplace.

In one’s own practice, it is essential to conduct thorough background checks of employees; maintain open lines of communication with nurses, bookkeepers and office managers; identify vulnerabilities in one’s system; utilize audit logs; increase one’s ability to react quickly to alleged misconduct; facilitate the payment of claims; reduce errors, particularly in regard to CPT codes; and identify any physician self-referral conflicts.

If a sanctioned employee is hired, be aware that the provider or the provider’s organization also becomes ineligible to participate in a federally funded healthcare program.⁹

Computer-assisted coding (CAC) is “the use of computer software that automatically generates a set of medical codes for review, validation, and use based upon the clinical documentation of the healthcare practitioner.”¹⁰ CAC provides compliance with regulations,

---

⁹ Abelson, R. etal. Ibid
creates an audit trail, and the cost of the software is reimbursable if one is able to demonstrate meaningful use for 90 days before the end of 2014.\textsuperscript{11}

Audit logs track changes within a patient record chronologically by capturing data elements such as date, time, and user stamps for each update to an EHR. An audit log can be used to analyze patterns to identify data inconsistencies. Audit logs should always be operational and be stored as long as clinical records. They should never be altered.\textsuperscript{12}

Private practices and hospitals are not the only professionals subject to scrutiny. Recently, the Centers for Medicare and Medicaid Services (CMS) was called out by the OIG for failing to identify and investigate EHR fraud. The failure contributed to an estimated loss close to $250 billion loss.\textsuperscript{13} In other words, CMS evaluated EHR with the same integrity strategies as those used for paper health records. Therefore, CMS and its contractors have to change their program integrity strategies in light the EHR technology. In a November 13, 2014 letter to OIG, CMS administrator Marilyn Tavenon concurred that the agency needed to do more, and confirmed that it would comply in specific areas.\textsuperscript{14}

The report highlighted the two most common EHR documentation practices used to commit fraud: copy-and-paste and over-documentation. The vast majority of doctors use the copy/paste function of their EHRs and many doctors’ notes are merely copied text.\textsuperscript{15} Copy-and-paste technology allows the provider to submit healthcare information multiple times (sometimes called “cloning”), often failing to update data to ensure accuracy. Over-documentation is adding

\textsuperscript{13} McCann, E. \textit{CMS called out for EHR fraud failing}. Healthcare IT News. April 2014.
\textsuperscript{14} McCann, E. Ibid.
\textsuperscript{15} Ibid.
false or irrelevant documentation to create the appearance of support for billing higher-level services.\textsuperscript{16}

Inspector General Daniel Levinson and the Department of Health and Human Services’ report on CMS and its contractors revealed that they had adopted only a few program integrity practices to address vulnerability in which EHR elicited a speedy response from CMS. Since then, the Department of Justice and HHS have announced record-breaking monetary recoveries through their joint efforts to combat healthcare fraud.\textsuperscript{17}

Former Attorney General Eric Holder and HHS Secretary Kathleen Sebelius released the annual HSFAC Program report showing that for every dollar spent on healthcare-related fraud and abuse investigations through this program and others in the last three years, the government recovered $8.10, the highest three-year average return on investment in the 17-year history of the HCFAC program.\textsuperscript{18}

With returns like these, the federal government is encouraged to continue prosecutions. Holder sent a strong message to providers who would take advantage of a vulnerable population of patients: Such abuse will not be tolerated.

The Justice Department and HHS are operating Medicare strike forces in nine areas across the country. In FY 2013 the strike force, under the umbrella of Health Care Fraud Prevention and Enforcement Action Team (HEAT) created in 2009, recovered records in the number of cases filed (137), individuals charged (345), guilty pleas (234), and jury trial

\textsuperscript{16} Ibid.
\textsuperscript{17} Levinson, Ibid.
\textsuperscript{18} Nelson Bolin, J. Ibid.
convictions (46). The defendants charged in 2013 are spending an average of 52 months in prison.\textsuperscript{19}

In that same fiscal year, Justice Department officials opened 1,013 new criminal healthcare investigations involving 1,910 potential defendants. A total of 718 defendants were convicted of healthcare fraud that year.\textsuperscript{20}

It is clear that the federal and state governments are willing to aggressively and doggedly pursue fraud and abuse cases. The scrutiny will undoubtedly only intensify as the healthcare industry transforms and expands. Oral and maxillofacial surgeons are strongly encouraged to routinely monitor their EHR protocols, remain vigilant in their coding and billing, and be cognizant of evolving government regulations.

\textbf{Bibliography}


Fraud Hotline, 2009. Available at \url{http://www.sso/gov/org/hotline/index.htm}.


\textsuperscript{20} Pearson, B. Ibid.
