HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

June 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Using technical safeguards to thwart phishing attacks

an interview with Adam Greene

Partner, Davis Wright Tremaine

See page 16

By Robin Singh, MSc-Law, MBA, CFE

Compliance 101

Fraud: A cancer to the healthcare domain

» If fraudsters find an exploitable weakness in your new healthcare domain, it not only affects the dollar value but also the patient's health and record—permanently.
» Manage and cultivate an understanding of correct coding and resubmission for denials.
» Have a proactive approach to compliance and define adequate controls, roles, and relationships for multi-party interactions.
» Set various data points to remain abreast of current events in the healthcare facility and enforce disciplinary actions.
» Develop and implement strong processes for identifying and addressing risks/regulatory requirements, etc.

Robin Singh *(robinsingh002@yahoo.com) is Corporate Senior Compliance and Fraud Examiner at Abu Dhabi Health Services Government Company (SEHA) in Abu Dhabi, United Arab Emirates.* *www.whitecollarinvestigator.com* */in/whitecollarinvestigator* *@drobinsingh*

Around the world, hospitals and other medical facilities are suffering from a loss of revenue. Medical revenue can be damaged in a number of ways.


Singh

What hurts healthcare revenue?

Both internal and external fraud and dishonesty can impact the revenue of a healthcare provider or practitioner, and fraud can occur in a variety of manners. For example, internal fraud involves the intentional manipulation of billing by healthcare practitioners. This typically occurs when a provider charges for services that are coded to be more expensive, are not medically necessary, or never even occurred. This type of manipulation may also involve the payment of kickbacks. Unfortunately, such fraud can go on for years before it is discovered, typically either through a whistleblower or an audit.

The loss of healthcare revenue can also occur as a result of patient dishonesty. Whether it involves refusing to pay bills or lying about insurance coverage, patient dishonesty can cause a loss of revenue, resources, and time.

Revenue cycle overview

The Healthcare Financial Management Association (HFMA) defines "revenue cycle" as, "All administrative and clinical functions that contribute to the capture, management, and collection of patient service revenue."[1]

Among the most significant challenges faced by many medical facilities and healthcare providers today is justifying the need for information technology systems. Yet, revenue cycle management can play a vital role in preventing loss of revenue. Far more than simple billing systems, revenue cycle management (RCM) information systems cover a number of areas, including pre-service financial clearance as well as discharge billing and post-service billing.

Popular fraud schemes and their explanations

Some of the most popular types of healthcare fraud schemes include the following.

Billing for more expensive services

Under this scheme, the facility will falsely bill for more expensive services or procedures than were actually performed or provided. This is typically referred to as upcoding, which may also involve inflating the diagnosis code for the patient's visit. For instance, a patient might come into the facility reporting chest pain and the facility upcodes the diagnosis to a heart attack in order to generate more revenue, even if the patient did not actually suffer a heart attack.

Unbundling

In this scheme, each step of a procedure is billed as though it were a separate procedure. This scheme may also involve billing the patient multiple co-pays for services that were actually paid in full or prepaid under a benefit plan or managed care contract.

Identity theft

Identity theft is rapidly becoming a major concern in the healthcare industry. This can not only affect the credit ratings of patients, but also result in significant revenue loss for medical facilities and healthcare providers. Under this type of fraud, the perpetrator provides the name or identifying information of another individual, without that person's knowledge, in order to obtain medical services. Identity theft may also be used to submit false insurance claims. Even more concerning than the risk of revenue loss is the potential for medical identity theft victims to receive the wrong medical treatment. Victims of medical identity theft may also be at risk for discovering that their medical insurance benefits have been used up. Individuals who have been targeted for medical identity theft may be surprised to fail physical exams for their jobs as a result of a medical condition or disease for which they have never been diagnosed.

Misrepresenting physician's privileges

The thought of someone misrepresenting the identity of a physician is certainly frightening, but it does happen. Investigations into healthcare fraud have uncovered situations in which physicians signed insurance claim forms stating they provided services when, in reality, healthcare professionals with less training actually performed the services. Under this scheme, the insurance company would pay more for the services rendered by physicians with more training.

Individuals who have been targeted for medical identity theft may be surprised to fail physical exams for their jobs as a result of a medical condition or disease for which they have never been diagnosed.

"Privilege" is an "authority granted to a physician or dentist by a hospital governing board to provide patient care in the hospital. Clinical privileges are limited by the individual's professional license, experience, and competence. Emergency privileges may be granted by a hospital governing board or chief executive officer in an emergency and without regard to the physician's or dentist's regular service assignment or status."[2]

Healthcare institutions may allow a non-privileged physician to carry out tasks for which he/she is not licensed or certified. And in order to ensure the claim pertaining to the treatment is not denied by the payer, they might change the name of discharging physician, prior to coding. This can lead to gross negligence from the physician and from the facilities side.

Bypassing medical necessity

This type of fraud involves coding to compensate for a shortfall in what is termed "medical necessity," which refers to a type of code used by a payer who requests additional documentation. Minor adjustments may be made to ensure that a non-denial transaction is received. The key elements that can cause such a denial are:

- Lack of contractual scope of coverage,
- Whether the proposed treatment is consistent with professional standards of practice,
- Whether the treatment is a medical necessity or for the convenience of the physician, and/or
- Excessive cost.

Invariably the missing documentation can cause other denials also, such as duplicate denial. This problem does not end here; it spans its wings beyond the realm of imagination, such as denials caused due to performing services outside a physicians' specialty. This can only be resurrected if there is a close link/loop between the Revenue Cycle Management team and the physicians. A loop can continuously communicate with the physicians if a drug prescribed or a certain medical treatment is being constantly rejected by the payer.

Duplicate denials

Duplicate denials are yet another common form of healthcare fraud. Each year, numerous healthcare claims are denied as a duplicate service. This is often one of the most common billing errors in many medical facilities. This can occur by changing the payer information associated with a patient, which can lead the system to believe that it is a new transaction while it is an incorrect or a duplicate transaction associated with the same patient. The ability to detect such transaction depends on the type of system owned or configured by the payer.

Cash drawer misrepresentation for self-pay patients

As is the case in any other facility in which a cash drawer is used, medical facilities and healthcare providers are at risk for fraud committed by cash drawer misrepresentation. This problem most occurs when treating self-pay patients who pay their own bills rather than having claim forms submitted to an insurance company. By misrepresenting the amounts received to the cash drawer, the staff in a medical facility can easily defraud medical facilities of massive amounts of money. Today's systems are capable of detecting these transactions, but it all fails during the time of reconciliation if there is collusion.

Bypassing system definitions

Under this scheme, system definitions are bypassed in order to categorize an outpatient as an inpatient for the purposes of achieving a non-denial encounter. Because inpatient care is typically more expensive than outpatient care, this can result in staggering levels of fraud. For example, an outpatient may fit into the definition of daycare patient or a daycare patient may fit into the definition of inpatient.

Sharing patient information with third parties

Unauthorized sharing of patient information with third parties might seem innocent enough on the surface, but it can actually place

patients at significant risk for becoming victims of identity theft. Furthermore, this can also compromise a protected status (e.g., HIV positive, mental health treatment) and expose an individual to discrimination. Compliance officers should ensure they develop guidelines, such as Patient Information Security Guidelines that cover confidential/sensitive designation, de-identification of records, patient access to records, and external access to records. This additional level of protection of patient information may be necessary or desirable, because of the nature of the patient's identity (e.g., public figure, high-profile individual, an organ donor, a prisoner) who, either alone or in combination with their health condition, may be at higher risk for breach of confidentiality and for whom the consequences of improper use or disclosure may be greater.

Theft of time via overtime

An age-old practice, the theft of time by reporting overtime that never actually occurred, can cost medical facilities massive amounts of money each year. Nurses are the ones who are on the front lines when it comes to patient care, which can lead to needed or unnecessary overtime. This is an area where it is difficult to bifurcate and set an acceptable or unacceptable limit between business and patient care. This fraud has a double impact, which can lead to a gross misconduct. Overtime towards excessive patient care leads to depletion of budget on the one hand, and on the other hand, these unusual long hours can lead to lower productivity that may cause minor or major medical errors.

Vendor medical education junkets

Continuing Medical Education (CME) is critical for any healthcare staff, but it holds a string potential for kickbacks. Various vendors carry out CME trainings for physicians, but their objective is to provide not only education, but also a sales pitch for their own products. Physicians/healthcare staff receive an honorarium for their work to incorrectly refer patients (referrals). Compliance officers should ensure that these trainings do not carry an honorarium over a modest amount and the healthcare facility's staff do not receive any other gifts, or else it carries a strong risk of diversion. Such guidelines by a compliance officer should fall under American College of Physicians guidelines, which state, "acceptance by a physician of gifts, hospitality, trips and subsidies of all types from the health care industry that might diminish, or appear to others to diminish, the objectivity of professional judgment is strongly discouraged. As documented by some studies, the acceptance of even small gifts (such as pens and mugs) can affect clinical judgment and heighten the perception and/or reality of a conflict of interest."[3]

Not guarding physicians from the vendors offering gifts and trips

Healthcare staff holds the sole responsibility to treat their patients in a fair manner without any conflicts. Nowadays vendors (e.g., vendor providing specialized drug or medical equipment) have realized that facilities are low on budget for training due to economic factors, and thus provide expensive gifts and travel vouchers for healthcare staff in critical positions. This could be detrimental for a facility, because this can sway a healthcare staff's mindset in prescribing medications or procedures that might not be needed. It also has a direct impact on a patient's permanent records and their health. Today's compliance officers need to make a choice whether to allow their healthcare medical staff to go for such training—if the staff know that there is a very limited budget for training (or CME)—and to ensure that even though they take the training,

that staff are mindful to provide quality patient care without conflicts of interest. Compliance officers should set out policies, such as a code of conduct or standard of conduct prohibiting such interactions and travel.

What can you do to avoid or prevent healthcare fraud?

As complex as healthcare fraud can be, some simple steps can be used to keep healthcare costs in check and prevent fraud.

As compliance officers, it is best to ensure adequate policies and procedures to cover guidance on how we may:

- Use patient information;
- Disclose patient information and under what circumstances;
- Share information with patients;
- Maintain and destroy records information;
- Make electronic recordings of patient information;
- Ensure adequate electronic declarations (e.g., annual declarations, conflict of interest, vendor sponsorship, kinship declaration, etc.);
- Perform periodic surveys;
- Carry out proactive data analytics to analyze denials, aged trial balance, productivity, etc.;
- Train on policies (face-to-face or online refresher courses);
- Set and enforce expectations towards an individual's duty of reporting (i.e., whistleblowing helpline); and
- Create a strong liaison with managers to understand what is happening.

Although the Compliance department might be seen as a cost center, Compliance acts as an anti-body, which shields this domain from fraudsters. Healthcare fraud is a serious matter that can drive up the cost of healthcare for everyone. Taking the time to become informed about fraud schemes can help to keep this problem in check.

1. Oregon Health & Science University: Patient Business Services, Revenue Cycle. Available at http://bit.ly/1Qcu41N
2. *The Free Dictionary: Medical Dictionary*: Definition of "privileges." Available at http://bit.ly/1RZ9uHz
3. American College of Physicians: *Conflicts of Interest and Medical Practice*, page 177. Available at http://bit.ly/1RZ9zuQ