○ July | ○ 2015

Compliance for you

JULY NEWSLETTER EDITION

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER™
Office *of* Institutional Compliance

UNDERSTANDING THE AFFORDABLE CARE ACT

The 60 Day Rule - The Clock is Ticking!

Not surprisingly, payors for healthcare services expect to be returned any monies which a provider, hospital, etc. were paid but should not have received. These "overpayments" can result from a number of reasons, such as findings of upcoding (billing for a higher level of service than what is supported by the documentation), incorrect modifier(s) resulting in a higher level of reimbursement, services billed under the wrong provider, lack of medical necessity, among others. Often these overpayments are identified through routine billing compliance auditing, internal audit activities and/or billing compliance investigations.

In 2010, the Affordable Care Act established the requirement for a person or entity who has received an overpayment to report and return the overpayment within 60 days, i.e., the 60 day rule. One of the most important questions under the 60 day rule is when the overpayment is ***identified***, which starts the 60 day clock. At this time, the government has not clarified when overpayment identification occurs and has left it up to healthcare entities to determine reasonable expectations for their own operations. For HSC (per Billing Compliance policy 3.1 *Report and Return of Overpayments)*, an overpayment is considered identified on the date which is earlier of:

- The Provider's Signature Letter (letter signed by the provider stating he/she agrees with audit findings indicating an overpayment has occurred)
  or
- Thirty (30) days after the end of the calendar quarter in which the monitoring occurred. For example, if the monitoring occurred during the first calendar quarter (January – March), then April 30th would be the date the overpayment was identified for purpose of repayment. The 30 day period is sometimes necessary if a provider goes on vacation or leave to allow a reasonable time to get their signature upon their return. If the provider's signature is not obtained by the 30th day, the claim is considered an overpayment and processed for repayment.

Once the overpayment is identified, the department responsible for the original billing will initiate a charge correction by contacting the TTUHSC Business Office. The Business Office will then process repayment to the payor either as a refund or the payor may "recoup" the overpayment by deducting the amount due them from a future payment. Once the repayment is made, the 60 day clock stops.
So why is it important to comply with the 60 day rule? Under the False Claims Act (FCA), the Centers for Medicare and Medicaid Services (CMS) may impose penalties on any person or entity which knowingly submits or causes the submission of a false or fraudulent claim for payment to the Federal government. A false claim could be for any number of reasons as described above (upcoding, lack of medical necessity, billing for services not provided, etc.). CMS can consider not returning an overpayment as a *reverse* false claim because the provider is keeping money they were not supposed to have received. Financial penalties for a false claim (or reverse false claim) can be $5,500 to $11,000 per claim and repayment of three times the original payment, i.e., treble damages. The most severe penalty would be exclusion from participating in Medicare and Medicaid. Obviously, the FCA is a big stick for the government. And which all healthcare providers want to avoid. The TTUHSC Office of Institutional Compliance (OIC) is increasing monitoring and oversight of the overpayment process, working with both the Business Office and clinical departments to insure all identified overpayments are repaid within the 60 day period. U.S. Healthcare is the one of the most highly regulated industries in the world, with literally thousands of rules and regulations on every facet of healthcare. Compliance at TTUHSC is not limited to the work done by the OIC, but is a responsibility of all employees. Only through our joint efforts can TTUHSC avoid pitfalls that could result in financial penalties and reputational harm.

What the HIPAA Rule Says About Use of PHI for Educational Purposes

The HIPAA Privacy Rule became effective in 2003 to provide the establishment of standards for the privacy of individually identifiable health information. Most disclosures of protected health information (PHI) require a patient's written authorization. TTUHSC is faced with a variety of challenges to be compliant with the HIPAA Rule. One of those challenges is the issue surrounding the HIPAA Rule and its impact on the training of residents and medical students. The academic teaching environment presents unique challenges for the protection of patient PHI within the framework of being compliant with federal regulations. The following information provides guidance and answers common questions specifically related to PHI and HIPAA in the academic environment.

PHI and Education Purposes

Internal Use and Disclosure of PHI: Physicians and staff can use PHI, without a patient's written authorization, to teach medical residents, nursing students, and other clinical students or trainees in the classroom. According to the OCR, this type of activity falls under the categories of treatment, payment, or health care operations (TPO). PHI must stay within Texas Tech University Health Sciences Center and not shared outside of TTUHSC. The amount of PHI used must be the minimum amount necessary to conduct the training.

Example: When using an image of a knife wound or foreign object in an on-campus lecture, remove the patent's name, medical record number, dates, and any other information that could lead to the identification of the patient that is not necessary to the training.

External Use of PHI: Faculty, staff, residents or students cannot use PHI for external educational meetings/ presentations, case studies, articles, industry conferences/lectures, posters, fliers, or media purposes without the patient's written authorization.

A policy regarding the use and disclosure of PHI in the classroom will be published to provide further guidance surrounding this matter.

FAQ of the Month

(provided by the office of Civil Rights)

Question: Can health care providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?

Answer: Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high quality health care. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- Nurses or other health care professionals may discuss a patient's condition over the phone with the patient, a provider, or a family member.
- A health care professional may discuss lab test results with a patient or other provider in a joint treatment area.
- A physician may discuss a patients' condition or treatment regimen in the patient's semi-private room.
- Health care professionals may discuss a patient's condition during training rounds in an academic or training institution.

A pharmacist may discuss a prescription with a patient over the pharmacy counter or with a physician or the patient over the phone.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high quality health care.

Medical Necessity vs. Medical Decisions in E/M Levels

Medical Necessity simply means the diagnosis documented merits the level of investigation and treatment administered to the patient. CMS states the medical necessity of a service is the overarching criterion for payment in addition to the individual requirements of a CPT code. It would not be medically necessary or appropriate to bill a higher level of evaluation and management (E/M) service when a lower level of service is warranted. The volume of documentation should not be the primary influence upon which a specific level of service is billed. Section 1862(a)(1)(A) of the Social Security Act, Medicare will not cover services that "are not reasonable and necessary for the diagnosis or treatment of illness or injury or to improve the functioning of a malformed body member."

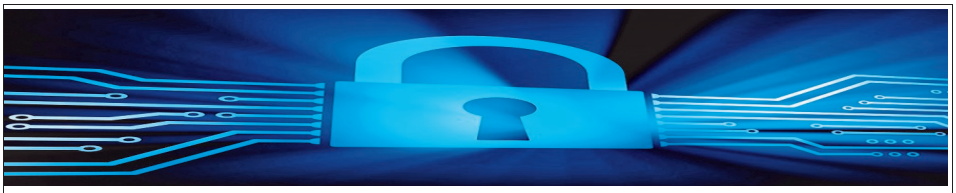
Each element of the history and physical exam is a separate procedure that should be performed only if there is a clear medical reason to do so. For example, for an established patient who complains of intermittent chest pain, it would be medically necessary to perform a comprehensive history to address this issue. And because the etiology of the chest pain is unknown, sound medical practice would dictate that a comprehensive exam may be performed to help guide the diagnosis and treatment.

On the other hand, when the same patient returns to the office for a follow-up visit six months after coronary artery bypass surgery with no specific somatic complaints, it would be difficult to justify a comprehensive history or exam. The extensive information obtained would not be helpful or clinically informative and therefore not within the bounds of medical necessity.

The point is to avoid payment denials or recouping money already dispersed that could result from a review of E/M records and a finding that they fail to substantiate either medical necessity for a condition or the level of medical decision making based on the actual physician effort in managing a diagnosis.

Family Practice Management, 2006 Jul-Aug; 13(7):28-32; "A Refresher on Medical Necessity." http://www.aafp.org/fpm/2006/0700/p28.html

---



Do you have Patient Information (PHI) on a portable device?

Theft of laptops or other portable devices such as smartphones, tablets, etc. that contain protected health information (PHI) are one of the most common causes of breaches of PHI. A portable device can contain information on thousands of patients, and if not properly protected through encryption, that information can be accessed to harm patients, financially and/or reputation. Healthcare institutions can also be fined up to $1.5 million by the federal government if found to not have taken sufficient steps to protect patient information.

It is TTUHSC policy that all portable devices (e.g., laptops, smartphones, tablets, etc.) containing electronic protected health information (ePHI) must be encrypted.

If you/ your department have portable devices with ePHI that have not been encrypted (or you are not sure), please call the IT Help Desk at 743-1234 to schedule a time to bring the devices by for an assessment and encryption if needed.

Compliance News!

Teri Murphy, Billing Compliance Director at the Amarillo campus, has passed the CPMA (Certified Professional Medical Auditor) exam and is now a Certified Auditor!

TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER
Office *of* Institutional Compliance

www.ttuhsc.edu/compliance
806.743.3949

www.ethicspoints.com
1.866.294.9352