MPC, Inc.
January 2017

CELEBRATING 24 YEARS OF EXCELLENCE

MEDICAL PRACTICE CONSULTANTS, INC

What the Government gives, they can take away!

The American Recovery & Reinvestment Act **(Recovery Act)** established Medicare and Medicaid electronic health records **(EHR)** incentive programs to promote the impletion and use of EHR. The goal was to improve quality and value to our healthcare system. With the incentive program came an obligation of a certain behavior by the health care provider as it related to the medical record.

CMS has stated that more than $30 billion has been paid in incentives by Medicare and Medicaid. According the Government Accountability Office (GAO) identified the highest risk to the program are the incentive payments made in error.

According to the Office of Inspector General (OIG) in the 2017 work plan, the following programs will be evaluated for errors. **As of July 2015, Medicare EHR incentive payments totaled more than $20 billion.** The OIG stated, “We will review Medicare incentive payments to eligible health care professionals and hospitals for adopting EHRs and CMS safeguards to prevent erroneous incentive payments. We will review Medicare incentive payment data to identify payments to providers that should not have received incentive payments (e.g., those not meeting selected meaningful-use criteria). We will also assess CMS’s plans to oversee incentive payments for the duration of the program and corrective actions taken regarding erroneous incentive payments.”

They further stated, “We will perform audits of various covered entities receiving EHR incentive payments from CMS to determine whether they adequately protect electronic health information created or maintained by certified EHR technology.”

OIG Incentive Programs

Under Review

Medicare Incentive Payments for Adopting Electronic Health Records—Medicare incentive payments are authorized over a 5-year period to physicians and hospitals that demonstrate meaningful use of certified EHR technology (Recovery Act, §§ 4101 and 4102). Incentive payments were scheduled to begin in 2011 and continue through 2016, with payment reductions to health care professionals who fail to become meaningful users of EHRs beginning in 2015 (§ 401b)).

Security of Certified Electronic Health Record Technology Under Meaningful Use—A core meaningful-use objective for eligible providers and hospitals is to protect electronic health information created or maintained by certified EHR technology by implementing appropriate technical capabilities. To meet and measure this objective, eligible hospitals must conduct a security risk analysis of certified EHR technology as defined in Federal regulations and use the capabilities and standards of certified EHR technology.

MEDICAL PRACTICE CONSULTANTS, INC.
Renee M. Brown, CEO, CMIS, ACS-EM, CHA
1900 NW Expressway, Suite 625
Oklahoma City, Oklahoma 73118
405/848-8558 or visit us at www.mpcinc.biz

Words of warning by the federal government of the systems we use daily and which may affect repayment in the future.

"While EHRs can improve health care delivery and provider services, they can pose provider challenges. **Challenges include, but are not limited to, privacy and security, author identification, altering entry dates, cloning, upcoding, and coding modifiers.** Further details on each challenge are explained in the following points:

Security and Privacy—EHRs can offer multiple improvements over paper documentation. **They can also pose security and privacy issues, such as allowing a malicious user to obtain patient information.** Providers should be aware of security features offered and utilize them when using EHRs. Security features include secure networks, firewalls, encryption of data, and password protection that ensures only appropriate or authorized entities can access certain information.

Author Identification—Different providers may add information to the same progress note. **When this occurs, each provider should be allowed to sign his or her entry, allowing verification of the amount of work performed and which provider performed the work.**

Altering Entry Dates—Be sure the EHR system has the capability to identify changes to an original entry, such as "addendums, corrections, deletions, and patient amendments." **When making changes, the date, the time, the author making the change, and the reason for the change should be included.** Some systems automatically assign the date an entry was made. Others allow authorized users to change the entry date to the date of the visit or service. Some systems allow providers to make undated amendments with out noting that an original entry was changed. **If there is no date and time on the original entry or subsequent amendments, providers cannot determine the order of events, which can impact the quality of patient care provided.**

Cloning—This practice involves copying and pasting previously recorded information from a prior note into a new note, and it is a problem in health care institutions that is not broadly addressed. For example, features like auto-fill and auto-prompts can facilitate and improve provider documentation, but they can also be misused. **The medical record must contain documentation showing the differences and the needs of the patient for each visit or encounter.** Simply changing the date on the EHR without reflecting what occurred during the actual visit is not acceptable. Using electronic signatures or a personal identification number may help deter some of the possible fraud, waste, and abuse that can occur with increased use of EHRs.

Upcoding—Upcoding, sometimes known as "code creep," occurs when a provider bills for a higher Current Procedural Terminology (CPT) code than the service actually furnished, resulting in higher payment. **Again, auto-fill and auto-prompts can facilitate and improve documentation, coding, and billing, but if used inappropriately, these tools may suggest a higher billing code and payment than the actual services furnished warrant, resulting in an improper payment.[** Claims paid without the appropriate supporting documentation are improper payments, and providers must return them.

Code Modifier—A modifier is an extension of an assigned code, such as a CPT code. Two reasons for using procedure codes include communicating the professional medical services performed and billing for the services provided. Modifiers are used in conjunction with codes to complete the picture of the procedures and services provided. More complex services may require additional modifiers. **When using modifiers, medical professionals should only use them to clarify the procedures and services performed and never for the purpose of increasing reimbursement."**

For full report by CMS go to: https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Downloads/docmatters-ehr-providerfactsheet.pdf

DO YOU KNOW YOUR OWN

**Medical Practice Consultants, Inc. can help you identify that risk. Please contact us at:
info@mpcinc.biz or call 405/848-8558.**