THE ACADEMY OF MEDICINE OF CLEVELAND & NORTHERN OHIO (AMCNO)
PRACTICE MANAGEMENT MATTERS

Spring Edition 2009

Red Flag Rule Becomes Effective on May 1, 2009 – Are You Ready?

In this issue – A New AMCNO Third Party Payor Review Form – if you have a problem claim fill out this form and return it with the pertinent information attached to our office for our assistance.

THE FTC'S NEW "RED FLAG" RULES: DO THEY APPLY TO MY PRACTICE?

On May 1, 2009, the Federal Trade Commission (FTC) will begin enforcing its so-called "Red Flag Rules," which require creditors to create and implement a written Identity Theft Prevention Program. The Rules went into effect on January 1, 2008, but enforcement of the Rules had been postponed to allow entities time to come into compliance with the regulations. The goal of the Rules is to attempt to minimize the incidents and impact of identity theft.

In creating these Rules, as an expansion to the existing Fair And Accurate Credit Transaction Act (FACTA), the federal government continues to recognize that identity theft can have a real and lasting impact on its victims. In the realm of healthcare, when an individual's identity is stolen, more than financial repercussions can occur. For example, false and inaccurate medical histories may be created leading to inappropriate treatment and/or denial of health insurance claims or coverage.

Despite the admirable goal of the Rules, there has been some push in the medical community to seek an exemption from the Rules for healthcare providers. However, at the moment, the FTC has taken a firm stance that there is no industry-based exemption to the Red Flag Rules. Additionally, the FTC has clarified that HIPAA compliance and maintenance of ethical obligations to protect patient confidentiality do not relieve healthcare providers from compliance with the Red Flag Rules.

Because of the broad definition of "creditor" under the Rules, many healthcare providers, even those with small practices who do not seem to extend credit in the traditional sense, may still be subject to the Rules. Consequently, the impending enforcement date leaves many healthcare providers scrambling to find out what needs to be done to come into compliance with the Rules.

Are You Subject To The Rules?

The first step in faring your way through the Red Flag Rules is to determine if you, or your practice, extend "credit" for accounts used primarily for personal, family or household services; i.e. patient accounts for medical care. "Credit" is defined basically as deferring payment for products or services. But what does this mean for healthcare providers? In short, payment plans constitute deferral of payment and are, therefore, an extension of credit. And, according to the FTC, even deferring payment to allow a claim to be submitted to the patient's insurance and billing the patient later constitutes extending credit, regardless of whether it is done as a courtesy to the patient or because it is required under contractual or state law. Therefore, if your practice utilizes payment plans or postpones payment in order to submit claims to insurance, it is likely that you must comply with the new Rules.

What Now?

Fortunately, the Red Flag Rules, and indeed the FTC, recognize that businesses, including medical practices, are not uniform. The Rules allow leeway for businesses to design and implement an identity theft protection program that is appropriate to its size, complexity, and the nature of their business. In fact, the FTC has stated that it expects that businesses for which the risks of identity theft are "minimal or non-existent will have a very low burden under the Rules." For example, a small medical practice with a well-known, limited patient base might have a lower risk of identity theft, and thus may adopt a more limited identity theft program than a clinic in a metropolitan setting that sees a high volume of new patients.

However, regardless of the size of your medical practice, basic steps need to be taken in order to comply with the Rules. You must assess the risk for identity theft in your practice, create a written program that identifies warning signs of identity theft (so-called "red flags"), implement a procedure to detect the "red flags," set forth a procedure to respond to "red flags" when they occur, and establish a schedule for periodic review of the program, updates, and personnel training.

Creating A Program

As previously discussed, an Identity Theft Prevention Program may be tailored to each healthcare provider based on the size, nature and scope of the practice. Generally, the Program will identify "red flags" of identity theft that may arise. Examples of "red flags" are:

- Alerts, notifications, other warnings received from consumer reporting agencies;
- Presentation of suspicious documents (e.g., obvious forgeries or physical descriptions or photos not matching the person providing the document);
- Suspicious personally identifiable information (e.g., fictitious addresses, inconsistent personal information; lack of correlation between SSN range and date of birth);
- Other suspicious activity on the account (e.g., suspicious change of address); and
- Notices from patients, victims of identity theft, law enforcement, or other persons regarding the possibility of identity theft in connection with the account.

Once the "red flags" of identity theft are identified, the Program must set forth a plan to detect the "red flags." For example, a detection method may consist of checking photo identification at the time services are sought to ensure that individuals seeking medical treatment are who they represent themselves to be. Another approach may be to add a photo of the individual to the medical file upon the first visit and to compare such photo against subsequent persons seeking service under that name. Also, if patients provide their social security number, there are simple rules-of-thumb to detect SSNs that are invalid on their face based on the numbers composing the SSN. Larger practices may want to subscribe to commercial services that can screen for SSN validity.

Next, the Program must set forth an appropriate response procedure for when a "red flag" has been detected, so that the identify theft is prevented and/or its impact is mitigated. One starting point may be to ask patients to explain any discrepancies between conflicting personal information, such as when the address on the driver's license does not match the address given by the patient. Also, if it appears that a person seeking treatment is not the current patient for whom the personally identifying information corresponds; an appropriate response may be to notify the original patient and to refrain from commingling the medical information for the two individuals. Other responses may include changing security codes for external access to patient accounts and medical records, declining to open an account or closing and renumbering an existing account, and actively monitoring or notating specific accounts if the healthcare provider is notified by a patient of the potential for identity theft. Additionally, the Program should provide that collection on the account be stopped, if identify theft has actually occurred.

The Program should also provide for all detected "red flags" to be reported to a specific person, such as the chief practitioner, who would have the responsibility to take further action appropriate in the situation, such as

thoroughly reviewing the circumstances and notifying law enforcement authorities if there is credible evidence that identity theft has occurred.

Implementing The Program

After the Identity Theft Prevention Program is created, it must be approved, implemented, and administered. Under the Rules, the Program must be formally approved by the entity's board of directors. If there is no board, the approval should be made by the highest executive authority (i.e. the entity's president, management committee, or owner of a sole proprietorship). Also, the board of directors, an appropriate committee of the board, or a designated member of senior management must oversee, implement and administer the Identity Theft Prevention Program.

Furthermore, appropriate workforce training must occur, such as providing general training for all staff members and more extensive training on the Program for staff members charged with patient registration. It is recommended that the Identity Theft Prevention Program be made part of the initial training of all new staff members as well as part of annual training. Records that such training occurred should be kept by the employer.

The Program must also be periodically reviewed and updated based on the business' experience in encountering identity theft and based upon any changes to the size, nature and scope of practice. At least annually, staff should provide a written report to the board or designated senior management regarding significant incidents involving "red flags" and management's response, the effectiveness of the policy and procedures, and recommendations for change.

If a practice involves service provider arrangements allowing third-party access to patient accounts, such as outsourced billing, the healthcare provider must take some steps to ensure that the third-party complies with its own identify theft protection program. This oversight of service provider arrangements may be accomplished through mandating such requirements in service agreements.

Again, keep in mind that Identity Theft Prevention Programs under the new Red Flag Rules can and should be tailored to your practices' specific size, complexity and nature. Solo practitioners with minimal staff do not need to create the same type of program as would be required of hospitals or large clinics. What is required, however, is that healthcare providers follow each step listed above to create, implement, oversee, and periodically update an appropriate Program. Of course, if you should have any concerns as to whether the policy you are creating brings your practice into full compliance with the Rules, you should seek the advice of legal counsel.

To recap the Red Flag Rules:

Step 1: Assess whether your entity is subject to the regulation.

A healthcare provider is subject to the Red Flag Rules if the provider extends credit and maintains "covered accounts". Credit includes deferring payment for services to a later date. A "covered account" is defined as an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions. Patient accounts are accounts for personal purposes and if multiple payments can be made on the account, the FTC considers it a "covered account" under the Red Flag Rules.

Step 2: Draft and Implement an Identity Theft Protection Program

Entities subject to the Red Flag Rules must design and implement an identity theft protection program which does the following:

1.) *Identifies Covered Accounts.*

2.) *Identifies Red Flags* - "Red flags" are warning signs of identity theft. Some types of "red flags" are:

- Alerts, notifications, other warning received from consumer reporting agencies;
- Presentation of suspicious documents (e.g., obvious forgeries or physical descriptions or photos not matching the person providing the document);
- Suspicious personally identifiable information (e.g., fictitious addresses, inconsistent personal information; lack of correlation between SSN range and date of birth); and
- Other suspicious activity on the account (e.g., suspicious change of address).

3.) *Detects Red Flags* – the Program must contain reasonable approaches to detecting the identified "red flags." One example would be instituting a policy to verify the patient's identity at time of registration.

4.) *Responds to Red Flags* – the Program must set forth a process to prevent and mitigate the damaging effects of identity theft through appropriate responses to "red flags". Examples of appropriate responses may be:

- monitoring covered accounts for evidence of identity theft;
- contacting the patient or account holder;
- changing security codes for external access to patient accounts and medical records;
- declining to open an account or closing an existing account; and
- notifying law enforcement.

5.) *Provides for administration of the program, periodic updates, and employee training.*

Step 3. Approve the Program

The entity's board of directors or other appropriate committee thereof must approve the Program. Also, either the board of directors or a senior level employee must be involved in the oversight, development, implementation, and administration of the program.

Further Information
Once again, it is recommended that entities consult with legal counsel to determine if they are subject to the Red Flag Rules and to create and implement a program in compliance with the Rules; therefore, physicians are encouraged to contact their legal counsel regarding this issue. **In addition, a sample form for use by your office is included at the end of this newsletter. If you have questions regarding the "Red Flag Rules," you may contact your own legal counsel or Ms. Heather R. Baldwin Vlasuk at the law firm that prepared this information for the AMCNO – Walter & Haverfield, LLP - (216) 781-1212.** Additional information on the Red Flag Rules and identify theft may be viewed on the FTC web site at http://www.ftc.gov/bcp/edu/microsites/idtheft// In addition, the FTC has prepared a guide for businesses – to view this guide go to http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus69.pdf

Medicare

Effective March 1, 2009: Tax Identification Number Required for Calls and Written Inquiries
Effective March 1, 2009, when you call either the IVR system or a Provider Contact Center (PCC) CSR, you will be required to provide three data elements for authentication: 1. Your National Provider Identifier (NPI); 2. Your Provider Transaction Access Number (PTAN); and 3. The last 5 digits of your tax identification number (TIN). This change is being made to better safeguard providers' information before sharing information on claims status, beneficiary eligibility, and other provider related questions. Please make sure that your staffs are aware of this new additional requirement for provider authentication.

New Advance Beneficiary Notice of Noncoverage (ABN) Form: Required as of 3/1/2009

Effective March 1, 2009, the only acceptable form for Advance Beneficiary Notices will be the revised ABN (CMS R-131). This new form combines the general Advance Beneficiary Notice (ABN-G) and laboratory Advance Beneficiary Notice (ABN-L) into a single form. The revised form also incorporates the Notice of Exclusion from Medicare Benefits (NEMB) form.

CMS Announces Regulatory changes in Change Request 6310.

On March 13, 2009, CMS released Change Request 6310 announcing the incorporation of regulatory changes. Said changes include, but are not limited to: (1) rejections and denials of certain physician and non-physician practitioner CMS-855 applications; (2) effective dates of CMS-855 applications submitted by physicians and certain non-physician practitioners; (3) timeframes for reporting CMS-855 changes of information; (4) licensure and educational requirements for certain types of non-physician practitioners; and (5) revocation effective dates.

For more information on any of the above referenced items go to the PalmettoGBA web site at www.palmettogba.com

Bureau of Workers Compensation

BWC Launches Web-Based Training for Medical Providers

The Ohio Bureau of Workers' Compensation (BWC) has launched a series of informational online videos created for BWC's medical provider network. The videos are intended to orient newly certified medical professionals with BWC's systems and processes, and to enhance their overall knowledge of the workers' compensation system.

The tutorials are the result of an initiative by BWC's Medical Services Division to more effectively serve the provider community and expand outreach to recruit and maintain a pool of topnotch providers. The nine videos currently available cover a number of topics, including:

- Intro to Workers' Comp for Medical Providers;
- Completing the First Report of Injury;
- Completing the Physician's Request for Medical Service or Recommendation for Additional Conditions for Industrial Injury or Occupational Disease;
- Completing the Request for Temporary Total Compensation;
- Completing the Physician's Report of Work Ability;
- Navigating the Medical Providers section of ohiobwc.com and creating an e-account;
- General billing instructions and commonly accepted billing forms;
- Alternative Dispute Resolution & Medical Billing Dispute Overview; and
- Frequently Asked Questions.

The videos are available for viewing at ohiobwc.com. The Medical Services Division is accepting feedback and suggestions for future topics at feedback.medical@bwc.state.oh.us.

Ohio Department of Insurance Provides Additional Information to Consumers and Providers

The Ohio Department of Insurance in collaboration with the AMCNO and other stakeholder organizations has created an electronic toolkit to assist with explaining the claim appeals process to consumers. Included in the toolkit are two newsletter articles targeted towards consumers and providers, a brochure and tip sheet, and a list of frequently asked questions.

The toolkit initiative – which includes helpful information for medical providers – was one of several topics to come from ongoing stakeholder meetings with representatives from the Department, insurance companies and associations, businesses, medical providers and consumer advocates inclusive of the AMCNO. They are working together to improve the prompt pay process in which doctors are reimbursed by insurers and how consumers can more easily appeal health coverage claim denials, and in particular, through independent review organizations (IROs).

In a news release to the media in the Northern Ohio area Elayne R. Biddlestone, Executive Vice President and Chief Executive Officer of The Academy of Medicine of Cleveland and Northern Ohio (AMCNO), viewed the stakeholder contributions as part of a team effort.

"We applaud the efforts of the Department to bring together key stakeholders to discuss improvements in the complaint review process," she said. "We also appreciate their decision to create the toolkit providing consumers and physicians with accurate and verifiable information that outlines their appellate rights under Ohio law. We look forward to working with the Department on other matters of importance to physicians and their patients."

The most recent stakeholders meeting on Jan. 22 focused on expanding the type of consumer complaint statistics provided by the Department, upgrades being made to the Department's provider prompt pay complaint database, an update on how the Department issues prompt pay data calls to health insurers and a potential expansion of the gathered data, an update on the Department's efforts to reform the availability and affordability of health insurance, and how consumers can be made more aware of the health claim denial external appeal process available through IROs. To view the items contained in the ODI toolkit go to http://ohioinsurance.gov/ConsumServ/healthcoverageappealtoolkit.htm

Practice Management Matters

The Academy of Medicine of Cleveland & Northern Ohio can provide you information on topics from balance billing to managed care to terminating the physician/patient relationship. The AMCNO Practice Management Department is available to address or investigate any claim issue as well. Call us at 216.520.1000 or email concerns@amcnoma.org *The AMCNO Practice Management Matters newsletter includes links that provide direct access to Internet sites other than our own. The AMCNO takes no responsibility for the content or the information obtained on other Web sites, as we do not have any editorial control over those sites. Additional information on these topics may be available on our Web site at www.amcnoma.org*

6100 Oak Tree Blvd· Suite 440 Independence, Ohio 44131

www.amcnoma.org

216·520·1000 Executive Offices 216·520·0999 Facsimile

Discounted Classes at Tri-C for AMCNO members

TRI-C Discount Programs for AMCNO: May-August, 2009

SEMINARS (CEUS: AAPC and PMI)

CPT Coding Fundamentals and More! 6 hours

Take advantage of this CPT coding seminar to strengthen your procedural coding skills and reduce your claims denials. In a hands-on, interactive session, you will work on multiple coding exercises with a focus on accuracy and compliance. Explore the construction of the CPT-4 Code book so that you truly understand how to use this reference guide. Coding scenarios will increase in complexity as the day progresses.

May 20th 9:00am-3:30pm Corporate College East $179

Auditing and Compliance Update for Coders 3 hours

This program is designed to give Coders, Business Managers, and Billing Staff an update on compliance activities both nationally and on the state level. New regulations and auditing activities will be reviewed.

Attendees will gain an improved understanding of new programs, rules, and compliance activities in Medicare and Medicaid. They will be able to utilize new tools and information to assess for potential compliance concerns

June 3rd 8:30am-11:30am Corporate College East $139

EVENING, DAY and WEEKEND CLASSES

Command Spanish for Nurses and Health Care Professionals-Wednesday Evenings

This nationally recognized program focuses on real Spanish for healthcare that can be used in a medical office.

Interact with Spanish-speaking patients and family members to improve patient care, customer service and avoid errors. This is not your typical Spanish class where the emphasis is on grammar. In fact, we promise-no grammar!

June 1st- July 29th (Wed evenings) Corporate College East 6:00-8:30pm $220

Get Certified in Professional Coding!

Accelerated AAPC Professional Medical Coding Curriculum-Saturday Mornings

This 36- hour program is formatted for the experienced coder summarizing the more basic concepts of the Professional Medical Coding Curriculum while emphasizing the more complex issues. Prepare for the CPC Certification Exam with this accelerated class.

Note: This course will require daily home-study. Current year CPT and ICD-9-CM Coding manuals required. AAPC Membership and Step by Step textbook included. *Prerequisite:* Students must submit letters from employers, verifying 2 years experience in medical coding. Bring letters to first day of class

May 30th-Aug. 1st Corporate College East 9am-1pm $850

The following classes are offered at various times and at various TRI-C campus locations. Call Linda Hale at the AMCNO for more information (see contact below).

Medical Terminology

Explore medical terminology, human anatomy, and methods for retaining the material. Review the structure and composition of the human body and organ functions while learning helpful methods for breaking down medical terms and meaning. Review word structure, visual identification of terms, spelling, definition, and pronunciations. Flash cards and CD-ROM practice to enhance comprehension of complex medical terms.

Note: Required textbook is "Medical Terminology: A Living Language" 4th Ed.
ISBN 978-0-13-158998-8

35 hours Offered at Corporate College East, Westlake and Metro-call for times $253

Medical Billing Reimbursement

Take this single course to enhance your billing skills, or take it as part of the Patient Access Specialist training program to prepare for your professional certification. Gain proficiency in insurance verification, eligibility and billing for Medicare, Medicaid and commercial insurance covered medical services. Engaging activities simulate procedures that are used by hospitals and other health care providers.

Note: Required Textbook is Medical Insurance An Integrated Claims Process Approach; ISBN 9780073256450 and the Workbook to accompany the text ISBN 9780073402109

24 hours Offered at Corporate College East and Metro Campus-call for times $282

To register: Call Linda Hale at AMCNO to obtain your Discount Promo Code at 216/520-1000.

THIRD PARTY PAYOR REVIEW FORM

The Practice Management Department of the Academy of Medicine of Cleveland & Northern Ohio (AMCNO) has been in existence for more than 20 years. When AMCNO members or their office staff has specific practice management issues, questions or concerns with the numerous insurance carriers, the practice management department is always available to address or investigate these and other issues. This third party payor review form is a tool physician offices may utilize when specific issues/problems with an insurance carrier arise.

Physician's Name: _____Specialty: _____

Address: _____

City: _____State: _____Zip: _____

Phone: _____ Fax: _____

Contact Person: _____Date Submitted: _____

Name of insurance carrier: _____

Address of insurance carrier: _____

Telephone number of insurance carrier: _____

CPT code in question: _____ Expected amount of reimbursement: _____

Patient First Name Only: _____ ***Insurance ID#: _____
(**Please do not include the patient's last name**)

Date of Service_____

Issue or Concern: (mark all that apply)

Types of Denials
Preauthorization
Referral
Claim

Payment Issues
Delay in payment
Late payment pattern
Pre/Post payment review

Claim Patterns
Down coding
Recording of claims
Lost claims
Data entry errors by insurer
Supporting documents missing
Pertinent claim information missing

Documentation Requests
Copy of medical record
Operative report

Telephone Access
Continuous busy signal
Excessive hold time
Numerous calls for a single claim
Other (specify) _____

Attach a letter describing the problem and detailing the sequence of events between your office and the insurance company. Also please attach copies of pertinent documentation including the claim, explanation of benefits, and any correspondence.

IMPORTANT: Please do not send confidential patient information without the proper patient consent. Remove all identifying information, such as patient's last name, from documentation prior to submitting to AMCNO. ***All claims must have a numeric

identifier as a form of identification. If the patient does not have an insurance identification number, use the primary policyholder's social security number or the patient's social security number. Please be advised that the AMCNO may share this information with the insurance carrier, relevant state agencies, or other parties to expedite resolution of your problem. The submission of this form and any attached information is consent to release this form and information, as appropriate, by the AMCNO. Please mail or fax this completed form to the **AMCNO, Practice Management Department, 6100 Oak Tree Blvd., #440, Cleveland, Ohio 44131 or fax (216) 520-0999.** If you have any questions regarding this form and its use or additional issues or concerns, please contact the practice management department at (216) 520-1000 or e-mail concerns@amcnoma.org