

**FEDERAL TRADE COMMISSION: “HEALTHCARE PROFESSIONALS ARE COVERED BY THE RULE”**

In a letter dated February 4, 2009 from Eileen Harrington, Acting Director of Bureau of Consumer Protection of the Federal Trade Commission to Margaret Garikes, Director of Federal Affairs, AMA, the FTC reiterated its previous stance that physicians and other healthcare providers who “regularly defer payment for goods or services” are covered under the applicability of the Identify Theft Red Flags Rule (“Red Flags Rule” or “Rule”).

As a brief background, the Rule is part of the Fair and Accurate Credit Transaction Act of 2003 (“FACTA”) which was developed partly in response to avert the increasing problem of identity theft.

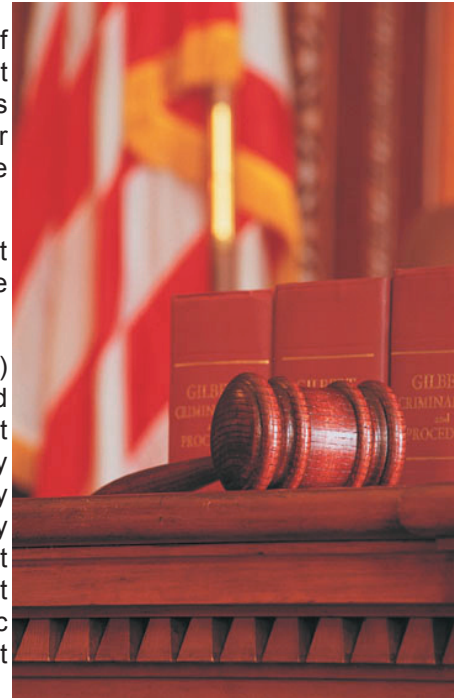
The Rule requires creditors and financial institutions (“covered entities”) to conduct periodic risk assessments to determine if they have “covered accounts” which includes any consumer type of account or other account for which there is a reasonable risk of identity theft. If the covered entity identifies such accounts, they must develop and implement a written “Identity Theft Program” to identify, detect, and respond to possible risks of identity theft relevant to them. The entities then must specify how they will detect the warning signs, aka Red Flags, that indicate an identity thief may be at work. It is suggested that, for example, the process might include periodic examination of patient’s accounts or detecting unusual patterns with respect to the use of an account.

The written Program must detail how to respond once the entity has detected a red flag. These responses might include refraining from billing the consumer whose identity was misused; or, making certain that the information related to the identity theft is not comingled with other information related to the victim (for example, medical records or consumer reports); and/or, reporting the incident of identity theft to a law enforcement agency.

Obviously, there is rightful concern about the increase of identity theft associated with fraud in the context of medical care. Medical identity theft has become common. The most frequent example is when an uninsured patient presents another person’s insurance card when attaining medical care. Charges for care are unknowingly submitted to the insurer in the name of a person not actually seen. This can result in not only false billing, but also the potentially life threatening corruption of a patient’s medical record.

Without belaboring this discussion by going into the definition of a “creditor” and the distinction that the FTC makes between high risk entities and low risk entities, suffice to say that many of the elements that are covered under the Red Flags Rule should have already been addressed in your practice under the auspices of the HIPAA Privacy and Security Rules. Indeed, the FTC points out that the Red Flags Rule generally compliments, rather than duplicates, the HIPAA data security requirements. And, as with HIPAA Security, the Rule is designed to be flexible and tailored to the degree of identity theft risk faced by the particular healthcare provider. In many cases, if that likelihood is minimal or nonexistent, a simple streamline program may be adequate. In fact, the FTC gives the example that for most physicians in low risk environments, an appropriate program might consist of checking photo identification at the time services are sought, and having appropriate procedures in place in the event the

*Continued on page 2*



**Inside This Edition**

<b>Federal Trade Commission “Healthcare Professionals are Covered by the Rule”.....</b>	<b>1</b>
<b>Some Good News in a Downturn Economy?.....</b>	<b>2</b>
<b>Changes In I-9 Form Due in April.....</b>	<b>2</b>
<b>FTC: “Healthcare Professionals are Covered by the Rule”.....</b>	<b>2</b>
<b>The ARRA and its Impact on HIPAA Privacy and Security.....</b>	<b>3</b>
<b>Kudos to Our Clients!.....</b>	<b>3</b>
<b>Company News.....</b>	<b>4</b>

## SOME GOOD NEWS IN A DOWNTURN ECONOMY?

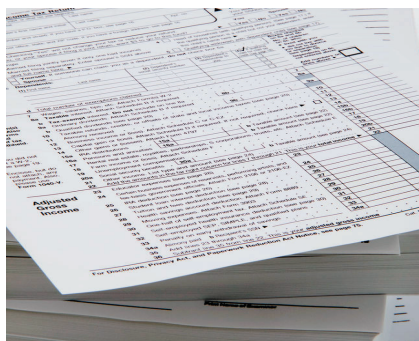


There may actually be some reassuring news that we can put in this edition of the Update that doesn't deal with regulatory issues. Information from recent meetings with various real estate developers indicates that now may be a wonderful time for you to look at opportunities to renegotiate your lease. This is particularly true if you have between 12 and 18 months left on your current lease. In many markets throughout the country, there is an abundance of medical office building space and other retail space that is suitable for medical tenants. Many owners are growing anxious to fill these vacancies. As they grow more anxious, they may offer concessions such as free rent for a period of time, leasehold improvement allowances, and significantly reduced rental rates.

One client in a suburban market was approached by a developer and encouraged to move their practice to a new medical office building in the same area in which they are currently located. The concession was a decrease of about \$3 per square feet in the actual lease rate for two years, as well as paying for the physical move (including rewiring of the telephone and computer systems) and even paying for the cost of reprinting stationary and other forms.

Somewhat reluctant to actually make the move, the client approached their current landlord and presented their options. The current landlord quickly responded with a reduction of \$4 per square feet for the next two years and a net decrease of \$2 per square feet for the following three years providing the practice with significant cost savings.

A word to the wise, it costs you nothing to engage a real estate broker. Generally they are paid their fees by the leasor. While you might think they have the tendency to want to seek a rich deal, in today's market, they are more interested in volume than they are a fat commission with every transaction. Now is a great time to start planning for the very near future if your lease is due soon.



## CHANGES IN I-9 FORM DUE IN APRIL

Since 1986, employers have been required to fill out an I-9 form within three days of hiring every new employee. In December 2008 the US Citizenship and Immigration Services (USCIS) announced a new form would become effective. After a slight delay, USCIS has indicated that employers should begin using the new I-9 form starting April 3, 2009.

What's so different about this form? It makes it very clear that employees can't use expired documents as identification and work verification. As well, it reduces the number of acceptable documents that employees can show for identification and work authorization purposes.

For more on the new I-9 rules, including a question and answer on the topic, go to: [www.dhrspcialist.com/i-9update](http://www.dhrspcialist.com/i-9update).

## FEDERAL TRADE COMMISSION "HEALTHCARE PROFESSIONALS ARE COVERED BY THE RULE"

[continued from page 1](#)

office is notified by the patient or law enforcement that the patient's identity has been misused.

*Gates, Moore & Company consultants are developing a written "Identity Theft Program" to assist you with implementing this Rule and hope to have it available in a short timeframe to meet the needs of our clients. Watch our website, [www.gatesmoore.com](http://www.gatesmoore.com), for updates.*

For related information, see the article on page 3 related to changes in the HIPAA regulations.

## THE ARRA AND ITS IMPACT ON HIPAA PRIVACY AND SECURITY

Since we know that most members of Congress didn't bother to read the 1,000 plus pages of the American Recovery and Reinvestment Act of 2009 (ARRA) (the "Stimulus"), we can likely assume that few of our readers have had time to read this all encompassing piece of legislation.

Through a set of provisions known as the Health Information Technology for Economic and Clinical Health (HITECH), the Stimulus extends the application of the main provisions of HIPAA Security and Privacy to a variety of different areas. The first of these that is of immediate importance is the expanded definition of business associates since it became effective on February 17, 2009, the date the act was signed. This expanded definition takes into consideration vendors who contract with covered entities to offer personal health records to patients. This includes entities that offer products or services through the website of a vendor of personal health records, entities that access or send information in a personal health record, and third party vendors of these entities. All Business Associates must comply with HIPAA Privacy and Security regulations.

One of the most important changes is that a covered entity that has a breach of protected health information (PHI) is now required to notify each individual whose "unsecured PHI has been, or is reasonably believed by the covered entity to have been accessed, acquired, or disclosed as a result of such breach". Further, there is the requirement for this notification to be made no later than 60 days after

the discovery of the breach. Specific guidelines are given as to how the notification must take place. More importantly is that in cases involving the breach of unsecured PHI of more than 500 individuals, notice must be provided to "prominent media outlets" serving the jurisdiction in which the breach took place. Also, the covered entity or business associate must notify the secretary of HHS who then in turn will post the information on the Department of Health and Human Services (DHHS) website identifying the covered entity involved in the breach.

There is also specific guidance included in the amendments to the original regulations that deals with electronic health information. Specifically, if a covered entity maintains electronic health information, then an individual has the right to obtain from the covered entity a copy of the information in an electronic format if they so choose.

The Act further expands the scope of enforcement to state attorneys general to bring civil action on behalf of their residents who they have reason to believe has been or is threatened or adversely affected by anyone who violates a provision of the act.

Finally, there has been further clarity given to the penalties that are connected with violations of the security and privacy standards. Specifically, there is a tiered penalty scale that ranges from at least \$100 per violation for unknowing violations to up to \$1.5 million for willful neglect compounded by the fact that the violation was not corrected in 30 days of the date the person liable for the penalty knew or should have known that the violation occurred. Moreover, the penalties associated with violation of HIPAA now expand to all business associates.

There are certain requirements that will not go into effect immediately but that the secretary is required to issue guidance on within eighteen months of the date of the enactment of the act.

Gates, Moore & Company consultants are working to improve and update our HIPAA Privacy and Security Manuals to include the new regulations as they have been enacted, and as they come on-line and further guidance has been issued.

### KUDOS TO OUR CLIENTS!

We are always pleased to acknowledge our clients for their successes and honors within the healthcare community.

**Richard M. Waldman, M.D.** has been named as the President Elect to the **American College of Obstetricians and Gynecologists**. Rich and his colleagues at Associates for Women's Medicine in Syracuse, New York have been clients for 10 years. We have been pleased to have the opportunity to interact with Rich not only in practice activities but also in ACOG activities throughout the course of the years.

**The Kennestone Heart Physicians Group** (Marietta, GA) has been rated by the Medical Group Management Association as a better performer for the second consecutive year. We are pleased to congratulate **Ross Berry, CEO** of KHPG for this wonderful accomplishment. Certainly to be recognized for the second consecutive year shows that Ross and his physician team are on the road to long-term success.



# Company News



## GATES, MOORE & COMPANY WELCOMES JOSH GREGG

**G**ates, Moore & Company is pleased to announce that we have hired Joshua W. Gregg as a staff accountant. Josh is a graduate of East Tennessee State University with a degree in Business Administration, concentration on Accounting. Prior to joining Gates, Moore & Company, Josh worked as a Business Office Specialist at Adventa Hospice in Tennessee, with an accounting firm in Tennessee, as well as a firm in suburban Atlanta. Josh has a great deal of experience with individual returns as well as with S and C corporation and partnership returns. He has also worked with the programs that many of our clients use for their daily write up activity.

Please join us in welcoming Josh as part of our great tax and accounting team.

## Update Newsletter Goes Green

The March 2009 Gates, Moore & Company Update Newsletter will be the last one to be printed and mailed. Do we have your e-mail address? If not, please email us with your name, practice name and email address [postmaster@gatesmoore.com](mailto:postmaster@gatesmoore.com) or go online to [www.gatesmoore.com](http://www.gatesmoore.com) to register electronically.



*We're going GREEN.*

*Update: Practice Management  
is published quarterly for clients by  
Gates, Moore & Company  
Your questions and comments may be  
directed to:*

*Gates, Moore & Company  
Tower Place 100, Suite 600  
3340 Peachtree Road, N.E.  
Atlanta, GA 30326*

*Phone: (404) 266-9876*

*Fax: (404) 266-2669*

*Email: [postmaster@gatesmoore.com](mailto:postmaster@gatesmoore.com)  
[www.gatesmoore.com](http://www.gatesmoore.com)*

PUTTING EFFECTIVE MANAGEMENT INTO PRACTICE

*Presort Standard  
U.S. Postage Paid  
Permit #6581  
Atlanta, GA*

*Gates, Moore & Company  
3340 Peachtree Road, N.E.  
Tower Place 100, Suite 600  
Atlanta, GA 30326*