Important Notice:
Ensure Your Compliance with the Red Flags Rule

On Dec. 31, 2010, the Red Flags Rule will be put into effect by the Federal Trade Commission (FTC). This policy requires health care practices to recognize the warning signs of identity theft through patterns, practices and specific activities. In addition, each practice must develop and implement a mandatory written identity theft prevention program. It is essential that Physicians follow the guidelines of this new federal regulation, as the FTC has established civil monetary sanctions of $2,500 for each incident of non-compliance.

Additional information on the Red Flags Rule, including compliance guidelines and resources for creating a theft protection program, is available in the *Doctors RX* – Volume 17, No. 2 Special Edition or by visiting the "Fighting Fraud with the Red Flags Rule" section of the FTC web site at: *www.ftc.gov/redflagsrule.*

Publication of Medical Mutual / Professionals Advocate®

DOCTORS RX

Volume 18, No. 1 Summer 2010

Medical Mutual Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company
Home Office: Box 8016, 225 International Circle
Hunt Valley, MD 21030 • 410-785-0050 • 800-492-0193

Publication of Medical Mutual / Professionals Advocate®

DOCTORS RX

Volume 18, No. 1 Summer 2010

A Letter from the Chair of the Board

Dear Colleague:

Since HIPAA and its related Privacy and Security Rules went into effect, there have been a number of new laws and regulations passed that further impact the day to day workings of Physicians and their practices. The Red Flags Rule (with a new compliance date of June 1st) as well as the new federal HITECH Act are among those that require your careful consideration and review.*

This issue of Doctors RX will highlight some of the key provisions of the HITECH Act and provide you with assistance in meeting the compliance goals that have been set forth in this new regulation.

George S. Malouf, Jr., M.D.
Chair of the Board
Medical Mutual Liability Insurance Society of Maryland
Professionals Advocate Insurance Company

** For more information on the Red Flags Rule, please refer to the article on the back panel of this newsletter.*

High Time for HITECH?
What Every Physician Needs to Know

Any Doctor who has been in practice since the 1990s is certain to recall the commotion that was caused by the enactment of the Health Insurance Portability and Accountability Act, better known as HIPAA. Since that time, compliance with privacy regulations has become almost second nature to health care providers. Despite the mainstream familiarity with HIPAA requirements, a heightened level of awareness is needed to tackle the demands of the new legislation.

The American Recovery and Reinvestment Act (ARRA), which was signed into law on February 17, 2009, contains significant changes to the privacy and security regulations to HIPAA. It also provides certain incentives for Physicians who adopt electronic health record (EHR) systems. These new provisions, which are contained in Title XIII of ARRA, are known collectively as the Health Information Technology for Economic and Clinical Health (HITECH) Act. The focus of this newsletter is to provide you with an overview of the HITECH Act and its impact on your practice.

Continued on next page

Susan M. Gordon, *BSN, JD*
James W. Saxton, *Esq.*,
Stevens & Lee P.C.

Reporting Breaches of PHI

The HITECH Act contains new reporting requirements with respect to breaches of medical record information, also known as protected health information (PHI). In general, the Act requires that patients be notified of any unauthorized uses and disclosures of their PHI.

Although the regulations were issued last August by the Department of Health and Human Services (HHS) and became effective as of September 23, 2009, HHS has stated that it would not impose sanctions for failure to provide the required notifications for those breaches discovered **before** February 22, 2010.

A *breach* is defined as the unauthorized acquisition, access, use or disclosure of unsecured PHI which compromises the security or privacy of such information. For purposes of this definition, "compromises the security or privacy of the PHI" means that the breach poses a significant risk of financial, reputational, or other harm to the individual.

For example: If the PHI contains Social Security numbers, license numbers or account information, the breach may pose a significant threat of identity theft and/or financial harm. A breach of protected health information that contains information indicating that a patient has cancer, a sexually transmitted disease, mental health issues, or other sensitive information may pose a significant risk of reputational harm.

Breach Notification

Following discovery of a breach of PHI, a Physician practice is required to notify each patient whose PHI was breached. If the breach involves 500 patients or more, then HHS must also be notified. In some situations, local media will need to be notified as well.

HHS is also imputing knowledge of the breach **to the practice** where an employee (other than the one committing the breach) has knowledge of the breach. Because of this, practices are required to ensure that their employees are adequately trained and aware of the importance of timely reporting of any privacy or security breaches when they become aware of them. Training may be provided in any number of ways including a formal educational program, or review of updated policies and procedures with each individual and a written acknowledgement of such training by the employee. This is particularly important for any new hires as part of their orientation training.

Notice of the breach is to be provided without unreasonable delay, but no later than 60 calendar days after discovery of the breach. This is the outside limit. The written notice is to be provided by first-class mail at the patient's last known address or by e-mail if the patient has previously agreed to electronic notice. Substitute notice by an alternative means must be provided if contact information is not available for the patient.

In order to determine whether a breach has triggered the notice requirements, Physician practices will need to undertake a two-step analysis:

1. Determine whether or not there has been access, use or disclosure of PHI that is not permitted under the Privacy Rule. **(Was there a breach?)**

2. Determine and document whether the impermissible access, use or disclosure compromises the security or privacy of the PHI. Such a determination will require a risk assessment by the covered entity. **(Does the breach create a significant risk of harm to the patient?)**

Not all breaches create a risk of harm. This is an analysis that needs to be made on a case by case basis.

Content of Notice

The notification must be written in plain language and is to include, to the extent possible:

1. A brief description of what happened, including the date of the breach and the date the breach was discovered, if that information is known.
2. A description of the types of information that were involved in the breach, such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other similar types of information.
3. The steps patients should take to protect themselves from potential harm resulting from the breach. For example, a practice might want to consider providing contact information for credit reporting agencies and information regarding placing a fraud alert on their financial accounts if the breach poses a significant risk of financial harm.
4. A brief description of what the practice is doing to investigate the breach, to mitigate harm to the patient and to protect against any further breaches (i.e. the practice provided additional training to employees, took appropriate disciplinary actions if they were warranted and revised its policies and procedures as necessary to prevent future breaches).
5. Contact procedures for individuals to ask questions or learn additional information. The contact information is to include a toll-free telephone number and either an e-mail address, web site or postal address.

In addition to the information that is required by the regulations, a practice should also provide reassurance to the patient that they are committed to maintaining the security and privacy of all patient information and they sincerely regret that the incident occurred.

Breaches by Business Associates

Business associates must notify the practice if the business associate is responsible for the breach. While the Physician practice is **ultimately** responsible under the rules for providing patients with written notice of the breach, the parties may determine which party will provide notice of the breach pursuant to their business associate agreement. Existing business associate agreements already generally provide that the business associate is obligated to provide notice of any breach of PHI. However, Physician practices might consider amending business associate agreements in order to clarify the definition of a breach; provide a description of what information must be provided to the practice regarding the breach; and ensure that a time frame is established to report breaches. If there are a large number of business associate agreements, the Physician practice will want to start with modifications to those where the risk of breach (or the cost of a breach) is highest.

Application of HIPAA to Business Associates

The HITECH Act provisions have very significant implications for business associates of Physician practices. Business associates are now directly subject to the HIPAA security regulations that require providers to adhere to certain safeguards to protect information, as well as the security rule requirement to implement written policies and procedures to comply with each of the safeguards described in the security regulations. The HIPAA civil and criminal penalties that apply to Physician practices that fail to comply with the privacy and security rules now apply directly to business associates. The practice may want to consider adding additional requirements to all business associate agreements to include the obligation of the business associate to maintain documentation of its administrative, physical and technical safeguards.

"Improved Enforcement" of Privacy Laws

The HITECH Act provides for "improved enforcement" of privacy laws and clarifies that the criminal penalties under HIPAA for violations are applicable to the individual employees of the practice who obtain or disclose patient information without the patient's authorization. Although HHS has recently announced that the enforcement of the business associate provisions of the HITECH will be delayed until final rules addressing the provisions are published, the HITECH Act provides increased civil penalties for noncompliance with the HIPAA privacy and security rules and fines now appear to be mandatory in all cases except those in the lowest of the tiered penalties.

- Tier 1 is for violations where the practice did not know and, by exercising reasonable diligence, would not have known that it violated a provision of the privacy or security rules. The penalty is at least $100 for each violation up to a maximum of $50,000 for each violation.
- Tier 2 is for violations that are due to reasonable cause and not to willful neglect. The penalty is at least $1,000 up to a maximum of $50,000 for each violation.
- Tier 3 is for violations due to willful neglect that are corrected within 30 days of the time the practice knew, or should have known of the violation. The penalty is at least $10,000 for each violation up to a maximum of $50,000 per violation.
- Tier 4 is for violations due to willful neglect that are not corrected within 30 days. The penalty is at least $50,000 per violation. The cap for all identical violations for all tiers is $1,500,000.

The HITECH Act also provides for enforcement of the HIPAA regulations by the State Attorneys General, who are permitted to bring civil actions in a U.S. District Court, obtain injunctions, and obtain damages on behalf of residents of the state. This is in addition to any enforcement powers the Attorney General has under state law. The court may award the costs of the action and attorneys fees in its discretion.

Civil penalties for noncompliance of the HIPAA privacy and security rules up through the present time have been almost nonexistent. The new law signals a clear intent on the part of the Federal government to begin assessing serious financial penalties for failure to meet the privacy or security standards set forth in HIPAA.

Incentives to Adopt Electronic Health Records

The government will invest over $19 billion of stimulus funds to promote and support the development of a system for the nationwide electronic exchange and use of health information. Hospitals and Physicians demonstrating "meaningful use" of electronic health record (EHR) technology and performance during the reporting period will be eligible for sizeable payment incentives.

To assist in the development of EHRs in Maryland, HHS recently awarded a $5.5 million dollar grant to a coalition of the Chesapeake Regional Information System for our Patients, MedChi, and the Community Health Integrated Partnership to create a Maryland Health Information Technology Regional Extension Center in the state. The goal of the Regional Extension Center is to facilitate and train Physicians to transition into electronic medical records, and better share and exchange critical health information. The grant's goal is to bring over 1,000 Physicians to "meaningful use" of electronic medical records in two years. For more information on this initiative, please visit *http://www.crisphealth.org.*

In Virginia, HHS awarded $24 million in federal funding to advance health information technology. The Commonwealth plans to use $11.6 million of the grant over the next four years to coordinate health IT initiatives through the establishment of an office of Health Information Technology. The remaining $12.4 million will be used to help Physicians acquire electronic health records for their practices. The latter initiative will be lead by the Virginia Health Quality Center, the Center for Innovation Technologies, Community Care Network of Virginia, and the Medical Society of Virginia. For additional information, Physicians can visit the MSV web site: *http://www.msv.org/MainMenuCategories/MemberCenter/Knowledgebase/HealthIT/Virginia-awarded-health-IT-grant.aspx*

Nationwide, Physicians who transition to EHRs may be eligible for Medicare incentive payments of 75% of their Medicare allowed charges, subject to the cap on applicable incentives for the year. The cap on incentives over a five year period is $44,000. Physicians with a significant number of Medicaid patients may be eligible for incentives up to $65,000 over a five year period. The Medicaid reimbursement will be managed at the state level. Many of the basic qualifications are similar to the Medicare program. Physicians will have to choose either Medicaid or Medicare; they cannot receive incentive payments under both programs. Physicians who are able to demonstrate "meaningful use" by 2011 or 2012 will be eligible for significantly higher incentives than those Physicians who delay implementation.

As currently written, meaningful use of EHRs includes capturing and tracking key clinical conditions for care coordination purposes, implementing clinical decision support tools, reporting clinical quality measures, utilizing computerized Physician order entry, electronic transmission of test results and use of patient self-management tools.

The Secretary of Health and Human Services will be providing further guidance to providers on what constitutes meaningful use by late spring 2010. It is hoped that once the details are made available, some of the more onerous requirements will be either changed or eliminated entirely.

HITECH Highlights:

Reporting requirements have expanded

- You will be required to notify patients of any unauthorized uses and disclosures of their PHI including breaches by your business associates

Review your Business Associate Agreements

- Ensure that your business associates have written security policies and procedures in place which include provisions to notify you of any breach of PHI and outcomes of their risk assessments
- In the event that the notice requirements are triggered, you would be responsible for providing the notification

Train your staff (Any of the following are acceptable training modalities)

- Staff may attend a formal educational program
- Office may conduct in-house review of policies and procedures to include a written acknowledgement of the training by each staff member
- It is also advisable to provide training as part of a new hire orientation (to include signed employee acknowledgement)

Know what to do in the event of a suspected breach of PHI

- Conduct a risk assessment to determine if notice requirements are triggered
- Determine if there was in fact a breach or if there was a permitted disclosure
- Determine and document whether the breach creates a significant risk of harm to the patient

Who to notify

- Each patient whose PHI was breached
- HHS (for breaches involving 500 patients or more)
- Local media (under rare circumstances)

How to notify

- ASAP but absolutely no later than 60 days after discovery of the breach
- Provide written notification to the patient's last known address via:

  - First-class mail (preferred method), or
  - E-mail if there has been prior consent to contact patient in this manner, or
  - If there is no contact information available you must attempt to provide notice by an alternative means

If you are interested in a copy of the Act, go to:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/hitechblurb.html
Be advised that many of its provisions have yet to be established and you should be on the lookout for future updates as they become available from HHS.

Summary

We have attempted to provide an overview of the scope of the combined HIPAA and HITECH regulations and the heightened expectation of compliance. Physician practices should continue to review and update their HIPAA privacy and security policies, and include procedures to address the breach notification requirements of HITECH. Practices should also update their business associate agreements to include language that reflects the new business associate requirements. MEDICAL MUTUAL and Professionals Advocate anticipate sending updated business associate agreements to their Policyholders by early summer.

For Physicians who wish to take advantage of the incentives for meaningful use of EHRs and avoid possible reimbursement cuts in the future, it will be necessary to adopt the use of an electronic health records system sooner rather than later. Regional Extension Centers will be a valuable resource for Physicians transitioning to EHRs.

Additional Resources
Maryland Healthcare Commission
http://mhcc.maryland.gov/electronichealth/electronichealth.html

Health Information Technology Spotlight (Virginia)
http://www.hits.virginia.gov/index.shtml

Doctors RX

Elizabeth A. Svoysky, J.D., *Editor*
Assistant Vice President – Risk Management

Dr. George S. Malouf, Jr., M.D., *Chair of the Board*
MEDICAL MUTUAL Liability Insurance Society of Maryland
Professionals Advocate® Insurance Company

Numbers you should know!

Home Office Switchboard	410-785-0050
Toll Free	800-492-0193
Incident/Claim/ Lawsuit Reporting	ext. 163
Risk Management Seminar Info	ext. 215 or 225
Risk Management Questions	ext. 224
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	www.weinsuredocs.com