Publication of Medical Mutual / Professionals Advocate®

DOCTORS Rx

Volume 21, No. 2 Fall 2013

A Letter from the Chair of the Board

Dear Colleague:

The passage of the 2009 HITECH Act brought about significant changes to the previously enacted HIPAA regulations. In the midst of these changes HHS advised that additional modifications to these regulations would be forthcoming. After much anticipation, HHS released the HIPAA Omnibus Final Rule in January of this year. The HIPAA Omnibus Final Rule not only clarifies the previous legislation, but significantly expands the accountability and enforceability of its provisions. This edition of* Doctors RX *serves as a concise overview of the key requirements of the HIPAA Omnibus Final Rule and provides a starting point for achieving compliance by the September 23, 2013 implementation date.

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

The HIPAA Omnibus Final Rule: What You Don't Know Can Hurt You

One need look no further than the daily paper or e-newsfeed to encounter sensational stories illustrating the detrimental effects a privacy breach can create for patients and the health care providers who have been charged with safeguarding patients' personal health information. Check out these all-too-common real life scenarios:

- Hospice group reaches a $50,000 settlement with HHS for failing to conduct a risk analysis and implement safeguards prior to the theft of an unencrypted laptop from an employee's car.
- More than 10,000 patient records compromised after the theft of an unencrypted portable device from an Arizona dental office.
- Idaho State University's Pocatello Family Medical Clinic reaches a $400,000 resolution agreement with HHS for failing to identify security vulnerabilities and establish review procedures that could have detected disabled firewall protections that resulted in the breach of approximately 17,500 patient records.

In this fast-paced, technology-driven environment we live in, privacy violations should be a concern for anyone involved in health care. While ensuring the privacy of an individual's health information is a worthy goal as well as a moral and ethical duty, achieving such a goal can prove

Continued on next page

Adrienne Shraibman, RDH, JD, CPHRM
Risk Management Specialist

to be a burdensome task. Novelist David Brin summed it up well – "When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else."

Did You Know?

- All privacy breaches, no matter how small **must** be reported to HHS on a yearly basis (or sooner for large scale incidents).
- The Final Omnibus Rule requires most health care providers to update their notice of privacy practices.
- Health care providers **must** comply with patient requests **not** to disclose PHI to health insurers for health care services paid entirely out of pocket.
- Business Associates and subcontractors are now directly liable for breaches they cause; however, that does not release the health care provider from liability for a breach by a business associate or subcontractor.
- In addition to civil monetary penalties ranging from $100 to $1.5 million, criminal sanctions, including imprisonment, may be sought for more serious violations.
- The names of those responsible for causing breaches involving over 500 individuals are publicly posted on the Health and Human Services website.

The Health Insurance Portability and Accountability Act (HIPAA), initially enacted in 1996, has been touted as the most significant legislation affecting the health care industry since the creation of the Medicare and Medicaid programs in 1965. Even though HIPAA has been in existence for 17 years, there remains considerable confusion concerning its interpretation and application. Much of the difficulty in achieving compliance has been attributed to the fact that the law is continually evolving. Only recently, the enactment of the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 (HITECH), brought about numerous changes to several key HIPAA provisions.

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) issued its final rule modifications related to HITECH that focuses on greater accountability of covered entities and their business associates for ensuring the security of patients' personal health information. This issue of *Doctors RX* will provide an overview of many of the key provisions of the Omnibus Final Rule, most of which have a compliance deadline of **September 23, 2013**.

Notice of Privacy Practices

Those Doctors who were in practice during the implementation phase of the initial HIPAA regulations will likely recall the near universal sense of confusion and frustration associated with incorporating the Notice of Privacy Practices (NPP) into routine business procedures. If you've reached the point where you finally feel like you've nailed down the requirements of the form and acknowledgement process, get ready – because change is on the horizon.

In a nutshell, the original rule required the NPP to describe the uses and disclosures of protected health information (PHI) a covered entity is permitted to make, the covered entity's legal duties and privacy practices with respect to PHI, and the individual's rights concerning his or her PHI.

The new Omnibus Final Rule requires a covered entity to make certain additional statements in the NPP, many of which are generally applicable to all covered entities, while others are dependent on the type of records maintained and/or the kinds of disclosures intended to be made. Fortunately, most of the changes are not terribly onerous to make; the primary difficulty being determining which statements are applicable to your particular situation.

The statements required to be added to **all** health care provider's NPP include the following:

- The right of the individual to be notified following a breach of unsecured PHI.
- The new right of patients to restrict certain disclosures of PHI to a health plan where the individual pays out of pocket **in full** for the health care item or service.
- Other uses and disclosures not otherwise described in the NPP will be made only with authorization from the individual.

The items below are statements that are **required** to be included in the NPP **if they apply** to your particular practice:

- Those health care providers who create or maintain psychotherapy notes (private notes of a mental health professional kept separately from the record) must include a statement that most disclosures of psychotherapy notes require patient authorization. The law does **not** require the health care provider to describe how these notes are recorded or stored.
- Health care providers who utilize patient information for marketing purposes must add a statement informing the patient that most uses and disclosures for marketing purposes, including subsidized treatment communications, will require the individual's authorization.
- Individuals may be contacted for fundraising purposes; however, the individual has the right to opt out of fundraising communications with each solicitation. The specific mechanism of the opt-out does not have to be included in the NPP, however each fundraising solicitation must provide the individual with the right to opt out.
- The NPP must include a statement that an individual's authorization is required for the sale of PHI. Most disclosures of PHI that constitute the sale of PHI will require the individual's authorization.

To lessen the administrative burden on health care providers, the government has clarified that covered entities that are health care providers are only required to distribute and obtain signed acknowledgement forms of the modified NPP to **new** patients. The law does not require acknowledgement of or mass distribution to **established** patients, but rather provides that a summary of the changes be conspicuously posted in the office and practice web site (if one exists) and copies be made available upon request.

Business Associate Direct Liability

Previously, a business that created, received, maintained or transmitted PHI as part of a business relationship with a covered entity had no direct responsibility to observe existing privacy laws except to the extent that the business may have contracted to do so with the covered entity. With the passage of HITECH, businesses, known as business associates, became obligated to comply with the administrative, physical and technical safeguard requirements of the HIPAA security rule. Included in the Omnibus Final Rule are a number of clarifications and expansions of the definition and responsibilities of business associates.

The Omnibus Final Rule affirms the business associate's responsibility to maintain compliance with many of the privacy and security provisions already required by HIPAA, and now explicitly provides for direct liability for violations by a business associate. This latest interpretation essentially imposes the same liability on a business associate as that of a covered entity. Although a business associate now has direct accountability and liability for violations, HHS has plainly stated that this in no way releases the covered entity from its own liability for the actions of a business associate.

To add to the confusion, the Omnibus Final Rule expands the definition of a business associate to include patient safety organizations, health information organizations, e-prescribing gateways, and persons who offer a personal health record to an individual on behalf of a covered entity. More importantly, the Omnibus Final Rule also designates downstream vendors such as subcontractors of a covered entity's business associates as business associates in their own right.

Consequently, business associates also will be required to execute a business associate agreement with their subcontractors. Due to the complexity of these relationships, it is highly advisable to review all of your existing business associate agreements to ensure that your business associates and their subcontractors have addressed issues such as: the implementation of appropriate safeguards; chain of reporting potential or suspected violations; and procedures for addressing violations.

Rest assured, as business associates, Medical Mutual and Professionals Advocate have obtained business associate agreements with you as our insureds, as well as with our subcontractors who may have access to PHI. Furthermore, we will continue to keep you apprised of any legislation that may affect these agreements in the future.

Modifications to the Breach Notification Rule

Undoubtedly, the most widely anticipated issue that the Omnibus Final Rule was slated to address was the reworking of the breach notification rule. As many expected, HHS implemented sweeping changes, not the least of which was the establishment of the **presumption of reportable breach.** Prior to the recent amendments, when a breach of PHI was suspected, the covered entity could perform an analysis of the risk of harm to the affected individual to determine if a breach was reportable.

The Omnibus Final Rule effectively eliminates this so-called "harm threshold," replacing it with a less subjective four-factor test to determine if the PHI has been compromised and if so, the need to report it to HHS. The four factors to consider are:

- The nature and extent of the PHI involved in the incident (e.g., did the disclosure contain sensitive information, social security numbers or test results);
- The recipient of the PHI (e.g., information received by another physician, who has his or her own ethical and legal duty to protect the information would be less problematic than someone else);
- Whether the PHI was actually acquired or viewed (e.g., was the information mailed in an envelope that was returned unopened as opposed to opened and resealed);
- The extent to which the risk has been mitigated following unauthorized disclosure (e.g., whether assurances of confidentially have been obtained and the data immediately destroyed).

Each of these factors focuses on the *probability that the data in question has been compromised* as opposed to what potential harm may be posed to the affected individual.

If the outcome of the analysis reveals more than a significantly low probability of compromise, then disclosure would be reportable to HHS, the affected individuals and possibly the media in the event of a wide-scale breach.

While the headlines that appear in the beginning of this issue of *Doctors RX* demonstrate catastrophic data breaches, don't be misled to believe that these are the only type of inadvertent disclosures HHS is concerned about. In fact, the rule specifically states that covered entities and business associates "make reasonable efforts to limit [the PHI] to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." Further, the guidance materials alluded to the potential of a breach determination in cases where more than the minimum necessary PHI to complete a transaction is disclosed – even in the context of a permitted disclosure.

The importance of conducting a risk analysis of your practice and updating your practice protocols for minimum necessary disclosure, document management, and breach analysis/response cannot be overstated, as some forms of breaches are almost inevitable.

Access to Electronic Medical Records

While it is important to recognize that HHS does not require a covered entity to purchase or utilize an electronic health record (EHR) system, it does, however, impose certain requirements for those that do. A covered entity that uses or maintains PHI in an EHR is now explicitly required to provide records in electronic format for those individuals who request it.

Whether providing the information via web-based portal, e-mail, or portable electronic media, covered entities must ensure reasonable safeguards are in place to protect the information. A few examples of this include: encrypting laptops and flash drives that house PHI; employing access and audit controls, such as ensuring restrictions on access to workstations; having unique user names and passwords; and scheduling periodic review of activity on electronic systems that contain PHI.

Regardless of whether paper or electronic format is used, health care providers may continue to charge a reasonable cost-based fee when providing access to medical records. Furthermore, the labor costs may include the actual cost of skilled technical staff time spent to create and copy an electronic file, such as compiling, extracting, scanning and burning the PHI to electronic media. The Omnibus Final Rule also provides for the cost of supplies for creating the paper copy or electronic media (CD, flash drive, etc.).

Patient Control Over Uses and Disclosures

The privacy rule previously required a covered entity to permit individuals to request restricted uses or disclosures of PHI under certain circumstances; however, a covered entity was not required to agree to the restriction. Under the Omnibus Final Rule, a covered entity **must** comply with a patient's request for a restriction on disclosure of PHI to a health plan for purposes of treatment, payment or operations for a service or health care item for which the provider was paid entirely out of pocket. While on the surface this may not seem to be a difficult allowance to make for patients, in practice it may prove to be one of the most technically problematic provisions to maintain compliance with.

One of the most challenging aspects of this requirement is the management of the information in re-disclosures. One example of this is providing follow-up treatment that is not paid for entirely out of pocket. HHS has stated that additional guidance on this issue will be made available although they have not specified precisely when this will occur. The advice provided in the guidance materials was primarily limited to encouragement for Doctors to maintain an open dialogue with patients so they have a better understanding of what disclosures may be required to process claims related to their care or follow up so that the patients can make decisions accordingly.

Interestingly, in the commentary of the Omnibus Final Rule, it was stated that health care providers will **not** be required to notify downstream providers (referrals, pharmacies, laboratories, etc.) of the fact that an individual has requested a restriction to a health plan.

Marketing and Sale of PHI

The Omnibus Final Rule "requires authorization for all treatment and health care operations communications where the covered entity receives financial remuneration for making the communications from a third party whose service is being marketed." The law does not distinguish between communications for treatment and those for health care operations purposes, but rather requires authorization for all subsidized communications that market a health related product. The Omnibus Final Rule further explains that authorization is also required for communications with a patient by a business associate or subcontractor who receives financial remuneration from a third party in exchange for marketing a health care product or service.

Financial remuneration includes both direct and indirect payment, but does not include non-financial benefits such as in-kind benefits provided to the covered entity or business associate for marketing the product or service. Notably, only payments made in exchange for the marketing communication require authorization. If payments are received by the covered entity for purposes other than encouraging the purchase or use of the product or service being marketed, than this marketing provision does not apply. An example of this would be if a third party provides payment to a covered entity to implement a program, such as a disease management program, the covered entity could make unauthorized communications to the patient about participation in the program. Another exception to the rule is subsidized face-to-face communications, although it is important to recognize that face-to-face communication does not include telephone or e-mail communications. Additionally, subsidized communications concerning drugs or biologics currently being prescribed to an individual and refill reminders may be made without authorization.

CME Evaluation Form

Statement of Educational Purpose

Doctors RX is a newsletter sent twice each year to the insured Physicians of Medical Mutual/Professionals Advocate.® Its mission and educational purpose is to identify current health care related risk management issues and provide Physicians with educational information that will enable them to reduce their malpractice liability risk.

Readers of the newsletter should be able to obtain the following educational objectives:
1) Gain information on topics of particular importance to them as Physicians,
2) Assess the newsletter's value to them as practicing Physicians, and
3) Assess how this information may influence their own practices.

CME Objectives for "The HIPAA Omnibus Final Rule: What You Don't Know Can Hurt You"

Educational Objectives: Upon completion of this enduring material, participants will be better able to:
1) Understand the key regulatory changes brought about by the HIPAA Omnibus Final Rule,
2) Identify provisions of the new rule that need to be addressed prior to September 23, 2013 compliance date, and
3) Implement policies and procedures and make necessary amendments to their notice of privacy practices.

	Strongly Agree				**Strongly Disagree**
Part 1. Educational Value:	5	4	3	2	1
I learned something new that was important.	❑	❑	❑	❑	❑
I verified some important information.	❑	❑	❑	❑	❑
I plan to seek more information on this topic.	❑	❑	❑	❑	❑
This information is likely to have an impact on my practice.	❑	❑	❑	❑	❑

Part 2. Commitment to Change: What change(s) (if any) do you plan to make in your practice as a result of reading this newsletter?

_____
_____
_____

Part 3. Statement of Completion: I attest to having completed the CME activity.

Signature: _____ Date: _____

Part 4. Identifying Information: Please PRINT legibly or type the following:

Name: _____ Telephone Number: _____

Address: _____
_____
_____
_____

CME Test Questions

Instructions for CME Participation

CME Accreditation Statement – Medical Mutual Liability Insurance Society of Maryland, which is affiliated with Professionals Advocate® Insurance Company, is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for Physicians.
CME Designation Statement – Medical Mutual Liability Insurance Society of Maryland designates this enduring material for a maximum of one (1) *AMA PRA Category 1 Credit.*™ Physicians should claim only the credit commensurate with the extent of their participation in the activity.

Instructions – to receive credit, please follow these steps:
1. Read the articles contained in the newsletter and then answer the test questions.
2. Mail or fax your completed answers for grading:

   Med•Lantic Management Services, Inc. Fax: 410-785-2631
   225 International Circle
   P.O. Box 8016
   Hunt Valley, Maryland 21030
   Attention: Risk Management Services Dept.

3. One of our goals is to assess the continuing educational needs of our readers so we may enhance the educational effectiveness of the *Doctors RX*. To achieve this goal, we need your help. You must complete the CME evaluation form to receive credit.
4. Completion Deadline: November 29, 2013
5. Upon completion of the test and evaluation form, a certificate of credit will be mailed to you.

1. All of the following are true about the changes to the notice of privacy practices EXCEPT:

   A. Must be redistributed to everyone
   B. Must include a statement of individual's right to be notified following a breach of unsecured PHI
   C. Must include a statement of the patient's new right to restrict disclosures to a health plan where the individual pays out of pocket in full for a health care item or service
   D. Must be made available on demand

2. Business Associates are now directly liable for breaches of unsecured PHI which they cause thereby eliminating the covered entities' liability for their business associates agreements.

   A. True B. False

3. All covered entities must provide patients with access to their records in electronic format, regardless of whether the records are maintained in an electronic format.

   A. True B. False

4. A covered entity must comply with a patient's request for a restriction of disclosure of PHI to a health plan for a health care service or item that the patient pays for entirely out of pocket.

   A. True B. False

5. HHS may impose fines for a covered entity's failure to perform a risk analysis of the practice and have policies and procedures to prevent, detect, and correct security violations?

   A. True B. False

6. The new rule on marketing communications distinguishes between subsidized communications for treatment and those made for health care operations purpose only.

   A. True B. False

7. Under the new breach notification rule the focus of the breach analysis is to determine the probability that the information has been compromised.

   A. True B. False

8. Covered entities are urged to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use.

   A. True B. False

9. The new rule addresses disclosures of immunization records for the purpose of school admission by eliminating the need for a written form so long as there is a documented oral agreement by the parent or guardian for the release.

   A. True B. False

10. Penalties for violations of the new rule are categorized into four distinct categories or tiers.

    A. True B. False

Decedents and Student Disclosures

While many of the provisions clarified in the Omnibus Final Rule require more work on the part of health care providers, there are some that serve to streamline the transfer of information. Two examples of these efficiencies are the amendments pertaining to the disclosures of decedents' PHI and release of students' immunization records.

Under the Omnibus Final Rule a covered entity may disclose health information to family members and other individuals who were involved in the deceased patient's care or the payment of that care, as long as the patient did not expressly disapprove of such disclosure during his or her life.

With respect to student disclosures, the Omnibus Final Rule eliminates the need for a formal written authorization form to release proof of immunization to a school for purposes of admission as long as there is a documented oral agreement between the covered entity and the parent or legal guardian of the student for the release.

A Brief Word on Penalties

A full evaluation of the impact of these amendments on Doctors as covered entities cannot be made without an understanding of the penalties for violations. To put it simply, the new enforcement provisions strongly reinforce the government's commitment to ensuring that the law is taken seriously. As such, four distinct categories of violations with increasing levels of culpability and fines have been established. Fines and penalties are based on the assessment by HHS of several factors – including the severity of the offense, whether the offense was known, the number of similar violations, and any attempts to correct the circumstances that caused the violation.

The dollar amount of these fines can range from $100 to $50,000 per violation up to a maximum of $1.5 million per calendar year for repeated violations. To further clarify, the fines may exceed the amounts listed above if different provisions of the law are violated within the same year. Additionally, in more egregious cases, the Department of Justice is empowered to impose criminal sanctions of up to ten years' imprisonment. The Secretary of HHS has broad discretion to waive all or part of any fine levied; however, in cases of willful neglect, penalties will be imposed.

In Conclusion

On March 26, 2013, the Omnibus Final Rule became law; however covered entities and business associates have 180 days beyond this date to fully comply with its provisions. As with any new law of this magnitude, it may seem overwhelming at first blush. This issue of *Doctors RX* was designed to promote awareness of the expansive nature of these changes and to encourage questions, as HHS advised that it will continue to provide guidance on how the Omnibus Final Rule is to be carried out in practice. While it is not possible to address every detail of the new legislation in one short publication, we hope this overview provides an easily negotiated first step in your journey toward compliance.

Compliance Tips

If you haven't done so already, consider the following:

- Evaluate your practice to determine which statements are required to be included in your NPP and amend the document for distribution.
- Update your business associate agreements taking into careful consideration whether or not the business associate is an agent and what safeguards the business associate has in place, including agreements with subcontractors.
- Perform a formal risk analysis of your practice describing known and potential security weaknesses and implement policies and procedures to prevent, detect, contain, and correct security violations. www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
- Develop a breach response plan.
- Review your policies and procedures regarding minimum necessary disclosures and protocols for the release of information within and outside of the organization.
- Determine if you conduct marketing, sale of PHI or research for which special authorization is required.

Additional Resources

Guidance on Information Security

www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule

www.nist.gov/healthcare/security/hipaasecurity.cfm

www.nist.gov

Website for Breach Notification

www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

The Final Rule: Modifications to HIPAA under HITECH

http://federalregister.gov/a/2013-01073

Doctors RX

Elizabeth A. Svoysky, J.D., *Editor*
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	800-492-0193
Risk Management Seminar Info	ext. 215 or 204
Risk Management Questions	ext. 224 or 169
Main Fax	410-785-2631
Claims Department Fax	410-785-1670
Web Site	mmlis.com proad.com

Compliance Audit Program Coming Soon!

As its pilot compliance audit program concludes, HHS is examining the data to develop a more efficient process, enabling them to increase the number of organizations reviewed. The results of the pilot program served to identify specific gaps in compliance that are responsible for the most breaches. The agency's preliminary review revealed that roughly two-thirds of pilot participants did not complete an adequate risk analysis. Consequently, it is likely that the permanent audit program will address whether an organization has conducted a truly meaningful risk analysis of their practice – one that thoroughly addresses high risk areas, is updated regularly as circumstances arise and justifies the rationale for the decisions made by the organization. Similarly, future audits will continue to focus on policies and procedures with emphasis on the manner in which these policies are actually implemented in practice. Having a policy in place is only the starting point as the agency will be looking to see if the organization is doing what it says it is doing. The permanent compliance audit program is anticipated to begin in October 2013.

Publication of Medical Mutual/Professionals Advocate®

DOCTORS Rx

Volume 21, No. 2 Fall 2013

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

PRST STD
U.S. POSTAGE
PAID
PERMIT NO. 5415
BALTIMORE, MD