The HIPAA / HITECH Omnibus Final Rule is Here! Is Your Health Care Organization Complying with the Rules?

(September 23, 2013): Effective **today**, all covered entities and business associates must comply with the Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule. Please keep in mind, the Final Omnibus Rule is **138 pages long.**

If you have not already read these new requirements, we strongly recommend that all covered entities, business associates and any affected subcontractors carefully review and adhere to these requirements. Summaries of these modifications may not fully address specific points which apply to your organization.

I. Overview:

The Omnibus Final Rule contains some of the most significant changes to the HIPAA Privacy and Security rules since their inception. The new rule also strengthens the ability of the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to enforce the rules and levy fines for any violations. The following article is intended to provide a brief synopsis of this new rule and outline how covered entities (such as your Physician Practice, Home Health Agency or Hospice) need to review their actions to better ensure that they are fully complying with the privacy, security and breach notification requirements which are now required.

II. HIPAA/HITECH Omnibus Final Rule:

On January 25, 2013, HHS issued a final rule[1] to modify the HIPAA Privacy, Security, and Enforcement Rules. This final rule implemented statutory amendments under the Health Information Technology for Economic and Clinical Health Act (HITECH) in order to strengthen the privacy and security protection for individuals' health information, modify the rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) under the HITECH Act, modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA), and make other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities.

More specifically, the final rule is comprised of four individual final rules. These rules:

1. Modify the HIPAA Privacy, Security, and Enforcement Rules mandated by the HITECH Act, as well as certain other modifications that improve the Rules. These modifications:

- Make business associates of covered entities directly liable for compliance with certain of the HIPAA Privacy and Security Rules' requirements;
- Strengthen the limitations on the use and disclosure of protected health information (PHI) for marketing and fundraising purposes, and prohibit the sale of PHI without individual authorization;

- Expand individuals' rights to receive electronic copies of their health information and restrict disclosures to a health plan concerning treatment for which the individual has paid out of pocket in full;
- Require modifications to, and redistribution of, a covered entity's notice of privacy practices (for examples, see **Section VI** below);
- Modify the individual authorization and other requirements to facilitate research and disclosure of child immunization proof to schools, and to enable access to decedent information by family members or others; and
- Adopt additional HITECH Act enhancements to the Enforcement Rule, such as the provisions addressing enforcement of noncompliance with the HIPAA Rules due to willful neglect.

2. Adopt changes to the HIPAA Enforcement Rule to incorporate the increased and tiered civil money penalty structure provided by the HITECH Act.

3. Finalize the Breach Notification for Unsecured PHI under the HITECH Act, which replaces the breach notification rule's ''harm'' threshold with a more objective standard.

4. Modify the HIPAA Privacy Rule as required by the GINA to prohibit most health plans from using or disclosing genetic information for underwriting purposes.

While the final rule took effect on March 26, 2013, all covered entities and business associates must comply with the applicable requirements of the final rule by September 23, 2013.

III. New HIPAA Rules Apply to Covered Entities and Business Associates:

Individuals, organizations, and agencies that meet the definition of a "covered entity"[2] under HIPAA must comply with the Rules' requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information.

More importantly, if a covered entity engages a "business associate" to help it carry out its health care activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate. This agreement must specifically state the work the business associate has been engaged to do and requires the business associate to comply with the Rules' requirements to protect the privacy and security of PHI.

In addition to these contractual obligations, business associates are directly liable for compliance with certain provisions of the HIPAA Rules. Specifically, business associates will be directly liable for:

- Impermissible uses and disclosures of individual PHI (including using or disclosing more information than is minimally necessary);
- Failing to comply with the Security Rule;
- Failing to provide breach notification to the covered entity, or, if a subcontractor, to the business associate above;
- Failing to provide electronic access as provided in the business associate agreement;
- Failing to disclose PHI to HHS in response to compliance and enforcement actions; and
- Failing to provide HITECH accounting, as necessary.

IV. What is a "Business Associate"?

A "business associate"[3] is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A business associate also

includes any subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate.

As discussed above, HIPAA Rules generally require that covered entities and business associates enter into contracts to ensure that the business associates will appropriately safeguard PHI. These contracts also serve to clarify and limit, as necessary, the permissible uses and disclosures of PHI by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose PHI only as permitted or required by its business associate contract or as required by law.

Importantly, a business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of PHI that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

V. Business Associate Agreements Between Covered Entities and Business Associates:

Based on the new rules, all covered entities should check to ensure that an updated business associates agreement between the covered entity and any business associates that they might have been put into place. It is appears that an updated business associate agreement has already been put into place, check it to ensure that it includes the following provisions:

1. Establishes the permitted and required uses and disclosures of PHI by any business associates;
2. Provides that business associates will not use or further disclose the information other than as permitted or required by the contract or as required by law;
3. Requires that business associates implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information;
4. Requires that business associates report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information;
5. Requires business associates to disclose PHI as specified in its contract to satisfy a covered entity’s obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings;
6. To the extent that a business associate is to carry out a covered entity’s obligation under the Privacy Rule, the agreement must require that the business associate comply with the requirements applicable to the obligation;
7. Requires that business associates make available to HHS its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity’s compliance with the HIPAA Privacy Rule;
8. At termination of the contract, if feasible, requires that a business associate return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity;
9. Requires that a business associate ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
10. Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between a business associate and other business associates (that are essentially subcontractors) must also be subject to these same requirements

If an updated business associate agreement has not been implemented, please take steps to have one completed immediately. A Sample Business Associate Agreement which incorporates the January 2013 changes has been published on OCR's website. Furthermore, the rules allow a business associate to continue to operate under existing business associate agreements up and until 09/22/14, under conditions that:

- Prior to the 01/25/13 publication date, the covered entity and its business associate had an existing written business associate agreement with prior HIPAA provisions; AND
- The business associate agreement has not been renewed or modified between the 04/26/13 effective date and the 09/23/13 compliance date.

VI. Notice of Privacy Practices (NPP):

If you have not already done so, it is imperative that you immediately update the "**Notice of Privacy Practices"** (45 CFR 164.520) being used by your practice or organization. To their credit, OCR recently published several examples of what they consider to be a ***"clear, accessible notice that. . . patients. . .can understand."*** OCR has published the following three examples that may be used by a covered entity to notify patients of their rights and the organization's privacy practices. These examples include:

NPP Booklet - HC Provider

NPP Layered - HC Provider

NPP Full Page - HC Provider

NPP HC Provider - Text Version

VII. The HIPAA Security Rule:

The HIPAA Security Rule[4] requires that covered entities implement "administrative, technical, and physical safeguards" to ensure the confidentiality, integrity, and availability of electronic PHI. The Rule also requires those entities to protect against anticipated disclosures and threats to the security of information. "Electronic PHI," or "*e*PHI" refers to all individually identifiable health information a covered entity or business associate creates, receives, maintains, or transmits in electronic form.

Under the new final rule, business associates are now directly liable themselves for complying with the Security Rule. Therefore, these organizations should review the Security Rule Guidance Material[5] provided by HHS and implement policies and procedures in much the same manner as a covered entity.

- **Security Risk Assessment**

Like covered entities, business associates must assess their security risks. A business associate must perform its own security risk analysis[6] to determine what the organization must do to address our security policies, procedures, and workforce training under HIPAA. The foundation for this process is compliance and is tailored to our legal practice. Our size, complexity, capabilities, in addition to the risks and costs to conduct this analysis and take appropriate action, has all been considered. This has allowed us to meet those standards that are "required" and determine whether an "addressable" standard applies. For this assessment, covered entities and business associates should broadly inquire into:

- Designing an appropriate personnel screening process;
- Identifying specific data that must be backed up and how we can execute that process;
- Implementing encryption methods for *e*PHI;

- Classifying what data must be authenticated in particular situations in order to protect data integrity;
- Designing written policies, procedures, and required notices; and
- Developing requisite training tools for these purposes.

Based on this risk assessment, your organization needs to implement certain security standards that can be divided into administrative, physical, and technical safeguards.

- **Administrative Safeguards**

The Omnibus requirements mandate that business associates implement administrative safeguards in compliance with the HIPAA Security Rule. Administrative safeguards[7] include “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”[8] Generally, these are the administrative functions that should be implemented to meet the fundamental security standards. They focus on workforce training and contingency planning.

Business associates should keep in mind that the most important administrative safeguards are risk analysis and risk management. Because both of these processes are “required," a business associate should execute a critical and thorough risk analysis before undertaking subsequent regulatory compliance measures. A business associate should also implement the following additional "required" administrative safeguards:

- Sanction policy for employee noncompliance.
- Tracking security "incidents" and documenting policies and procedures for dealing with incidents. Resulting harm must be mitigated.
- Appointment of a security officer.
- Allowing employee access to *e*PHI only where appropriate, and putting policies in place to prevent unauthorized persons from gaining access.
- Training employees on security issues, scaled to our organizational size.
- Implementing contingency plans for emergencies that damage systems with ePHI, including provisions for data backup, a recovery plan and a mode for continuing critical business processes for the protection of the security of *e*PHI during emergency operation.
- Ensuring that periodic evaluations of security preparedness are conducted.

Again, these standards and implementation specifications pertain to administrative functions, such as policy and procedures that must be in place for management and execution of security measures, and are just the first set of safeguards that have been implemented.

- **Physical Safeguards**

Physical safeguards[9] incorporate mechanisms, policies, and procedures required to protect electronic systems, as well as equipment and the data contained therein, from threats, environmental hazards, and unauthorized intrusion. These safeguards include restriction access to *e*PHI and retaining off-site computer backups.

Covered entities and business associates must ensure that *e*PHI and the computers which house that private information are protected from unauthorized access. Covered entities and business associates should also recognize that some of the requirements to be implemented as physical safeguards can be accomplished through the use of electronic security systems. Possible approaches include, but are not limited to:

- Establishing a policy for the appropriate use, physical attributes of and security for workstations that access *e*PHI.
- Establishing policies dictating the procedures for the addition, disposal, or reuse of hardware or electronic media that contains *e*PHI.

After successfully implementing these, and other, standards and protections, an organization will be able to protect those covered entities' *e*PHI from natural and environmental hazards, as well as unauthorized intrusion.

- **Technical Safeguards**

Finally, the new Omnibus Rule also requires that business associates implement technical safeguards[10]. Generally, these types of safeguards are the automated processes used to protect data and control access to data. For example, they include using authentication controls to verify that the person signing onto a computer is authorized to access that *e*PHI, or encrypting and decrypting data as it is being stored and/or transmitted.

Covered entities and business associates should review and implement the following "required" technical safeguards (as appropriate):

- Policies that limit software program access to only those with authorized access. Organizations should also provide their employees with unique log-ins and ensure that automatic log-offs cannot be utilized. Further, they should implement procedures for obtaining necessary *e*PHI during an emergency.
- Maintaining activity logs (or "audit logs") of all systems that contain *e*PHI.
- Policies to protect *e*PHI from alteration and destruction.
- Procedures to verify the identity of those seeking access to *e*PHI.
- Protection for the transmission of ePHI over a network through technical security policies.
- While encryption is only an "addressable" standard, a business associate should strongly consider using encryption to encrypt *e*PHI..

Importantly, each covered entity and business associate must also analyze their administrative, physical, and technical factors so that safeguards can be implemented to protect the integrity of PHI.

- **Documentation Requirements**

A proper risk assessment and all subsequent compliance measures must include proper documentation procedures. Therefore, a business associate must ensure that all compliance activities be documented accordingly and be retained for six years. Business associates need to recognize that policies and procedures are amendable as further regulations and policies require. Therefore, business associates should conduct periodic reviews of its policies, document those review, and take any appropriate actions when changes in the environmental security of *e*PHI are needed.

VIII. Business Associates and the Privacy Rule:

The HIPAA Privacy Rule restricts covered entities' use and disclosure of an individual's PHI. For example, providers who transmit PHI electronically in a HIPAA Standard Transaction, such as by filing electronic claims or checking eligibility electronically even if they are using a third party such as a billing service or clearinghouse, become a "covered entity". They are then bound by HIPAA and its requirements. Under the final rule, certain privacy changes have been enacted that impact business associates.

However, the HITECH Act does not impose *all* of the Privacy Rule obligations on business associates. A business associate is subject to direct enforcement of the HIPAA Privacy obligations and penalties in the same manner as a covered entity, but only to the extent required under the HITECH Act – not the HIPAA Privacy Rule itself.

Both covered entities and business associates must ensure that any disclosure of PHI is kept to limited data sets or minimum amounts of information as necessary. Furthermore, those covered entities that a company has a business associate agreement with must honor any and all requests by an individual to restrict disclosure of PHI to a Health Plan if the individual pays for the associated service out-of-pocket in full. The business associate must also acknowledge that the sale of PHI is prohibited unless authorized by the individual, and certain marketing communications require additional authorizations.

IX. The HIPAA Breach Notification Rule:

The Breach Notification Rule requires covered physician practices to notify affected individuals, the Secretary of HHS and, in some cases, the media when they discover a breach of a patient's unsecured PHI.

Business associates must now comply with breach notifications procedures under the new HIPAA Omnibus Rule. If a breach of unsecured PHI occurs, a business associate must notify the covered entity following the discovery of the breach. Discovery of a breach is when the business associate "knew or should have known" of the incident.

Furthermore, any business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, a business associate should also provide each covered entity with the identification of each individual affected by the breach, as well as any information required to be provided by the covered entity in its notification to the affected individual(s).

Under the new Omnibus rules, breaches are now presumed reportable unless, after an organization has completed a risk analysis, it is determined that there is a "low probability of PHI compromise." To conduct this analysis, covered entities and business associates must consider the following four factors:

1. The nature and extent of the PHI involved – an organization should consider issues such as the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
2. The person who obtained the unauthorized access and whether that person has an independent obligation under HIPAA to protect the confidentiality of the information;
3. Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
4. The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

Covered entities and business associates must keep in mind that this rebuttable presumption of breach and four-factor assessment of the "risk of PHI compromise" replaces HIPAA's previous, more subjective "significant risk of financial, reputational or other harm" safe harbor analysis for establishing a breach. The organization also understands that the new rules further clarify that there is no need to have an independent entity conduct the risk assessment and indeed, no risk assessment need be conducted at all if the breach notification is made. Nevertheless, a business associate must undertake an appropriate review and steps to mitigate the harm and reduce the likelihood of future breaches in any case as necessary.

Finally, both covered entities and business associates must implement ***"Breach Notification Policies and Procedures,"*** workforce training, and associated documentation procedures on how to document and handle breach incidents.

X. Government Audits:

Under the new rule, HHS will be performing audits to ensure that covered entities and business associates are fully complying with the HIPAA Privacy, Security and Breach Notification requirements. Notably, HHS-OCR, the federal agency within HHS with oversight over HIPAA privacy, security and breach notification requirements, has established a comprehensive audit protocol that should be considered during reviews and updates to their HIPAA compliance plans. The OCR audit protocol contains 170 audit areas (79 Security Rule, 10 Breach Notification Rule and 80 Privacy Rule provisions) covering all of the following:

- Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures;
- Security Rule requirements for administrative, physical, and technical safeguards; and
- Breach Notification Rule requirements.

The safeguards that covered entities and business associates ultimately implement should withstand the scrutiny of an HHS-OCR audit, if such an audit is ever conducted.[11]

XI. Penalties:

It is imperative that covered entities, business associates and their staffs understand that a failure to comply with HIPAA can result in significant civil and criminal penalties.

- **Civil Penalties**

The HITECH Act established a tiered civil penalty structure for HIPAA violations. The Secretary HHS still has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. Nevertheless, the Secretary is still prohibited from imposing civil monetary penalties (CMPs) (except in cases of willful neglect) if the violation is corrected within 30 days (a time period that may be extended). Furthermore, HHS may waive a CMP in whole or in part in some situations. Moreover, HHS's authority to impose a civil money penalty is prohibited if a criminal penalty has been imposed.

HIPAA Violation	Penalty Range	Annual Maxim
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA.	**$100 - $50,000 per violation**	**$1.5 million**
Individual "knew, or by exercising reasonable diligence would have known" of the violation, but did not act with willful		

neglect.	**$1,000 - $50,000 per violation**	**$1.5 million**
HIPAA violation due to willful neglect but violation is corrected within the required time period.		
	$10,000 - $50,000 per violation	**$1.5 million**
HIPAA violation is due to willful neglect and is not corrected.		
	$50,000 per violation	**$1.5 million**

Under the new HIPAA Omnibus Rule, HHS must conduct a formal investigation and impose civil monetary penalties in cases involving willful neglect. HSS may also provide PHI to other government agencies for enforcement activities. The assessment of penalties must be based on five principal factors:

1. The nature and extent of the violation, including the number of individuals affected,
2. The nature and extent of the harm resulting from the violation, including reputational harm,
3. The history and extent of prior compliance,
4. The financial condition of the covered entity or business associate, and
5. Such other matters as justice may require.

The number of violations may be based on the number of individuals affected or by the number of days of non-compliance. Finally the HIPAA Omnibus Rule clarifies that the 30-day cure period begins when the individual knew or should have known of the violation.

- **Criminal Penalties**

Both covered entities and business associates must recognize that criminal penalties under the new Omnibus Rule are quite severe. Covered entities and specified individuals, as outlined below, whom "knowingly" obtain or disclose individual PHI in violation of the HIPAA requirements face a fine of up to $50,000, in addition to imprisonment up to one year. Furthermore, offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm permit fines of $250,000, and imprisonment for up to 10 years.

- **Covered Entity and Specified Individuals**

The DOJ has determined that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, health care clearinghouses, health care providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of "corporate criminal liability." Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

- **Knowingly**

The DOJ interprets the "knowingly" element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.

- **Exclusion**

HHS has the authority to exclude from participation in Medicare any covered entity that was not compliant with the transaction and code set standards by October 16, 2003 (where an extension was obtained and the covered entity is not small.[12]

- **Enforcing Agencies**

The HHS OCR enforces the privacy and security rules, while the Centers for Medicare & Medicaid Services (CMS) enforces the transaction and code set standards.

- **No Private Cause of Action**

While HIPAA protects the health information of individuals, it does not create a private cause of action for those aggrieved (meaning an individual cannot take legal action against a covered entity for a HIPAA violation based on the HIPAA law). State law, however, may provide other theories of liability.

XII. Conclusion:

The new HIPAA Omnibus Rule includes a set of final regulations modifying the HIPAA Privacy, Security, and Enforcement Rules to implement various provisions of the HITECH Act. These rules are quite complex and mandate numerous new policies, procedures, and safeguards that both covered entities and business associates must implement in order to safeguard individuals' PHI. Both covered entities and business associates must thoroughly analyze the risks involved with maintaining and protecting the PHI they receive from patients (in the case of covered entities) and from covered entities (in the case of a business associate), so that they can fully comply with applicable statutory and regulatory requirements.

Robert W. Liles is Managing Partner at the health law firm of Liles Parker PLLC. Our firm represents physicians, home health agencies, hospices, skilled nursing facilities and other health care providers around the country in connection with HIPAA, compliance and a full range of other health care transactional projects. Should you have a question, please feel free to give us a call. For a complimentary initial consultation, please call Robert at: 1 (800) 475-1906.

---

[1] **http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf**

[2] See 45 CFR 160.103 for the definition of a “covered entity”.

[3] See Id.

[4] See 45 CFR 160 and 164.

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

[6] A business associate may utilize NIST SP 800-30 as an initial starting point.

[7] See 45 CFR § 164.308 for more detailed information on administrative safeguards.

[8] 45 CFR § 164.304

[9] See 45 CFR § 164.310 for more detailed information on physical safeguards.

[10] See 45 CFR § 164.312 for more detailed information on technical safeguards.

[11] HHS OCR’s HIPAA Audit Program Protocol is available at **http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html.**

[12] 68 FR 48805