TILLONA LAW LLC

LAW NEWS

FINAL OMNIBUS HIPAA/HITECH RULES
and their Imapct on Business Associates

By Mary Anne Tillona
mtillona@tillonalaw.com
March, 2013

Summary

On January 25, 2013, the Department of Health and Human Services ("HHS") published final omnibus rules (the "Final Rules")[1] which adopt "sweeping changes" to the HIPAA Privacy, Security and Enforcement Rules and the breach notification rule under the Health Information Technology for Economic and Clinical Health Act ("HITECH") and strengthen privacy and security protections for individuals' health information.

The Final Rules will have a material effect on Business Associates. This article summarizes the key provisions affecting Business Associates. Principally, the entire HIPAA Security Rule and much of the HIPAA Privacy Rule now apply directly to Business Associates and their subcontractors. Business associate agreements are required to contain certain provisions which may necessitate modification.

The Final Rules also address privacy issues concerning a number of specific types of uses or disclosures of protected health information ("PHI"). These include communications for marketing and sale of PHI.

With regard to security breaches, the Final Rules eliminate the "harm threshold" that required notice to the Covered Entity and HHS of an unauthorized use or disclosure of PHI if the use or disclosure posed a significant risk to the affected individuals. In its place, the Final Rules provide that *any* use or disclosure of PHI that is prohibited by the Privacy Rule will be presumed to be a reportable breach. Business Associates can rebut this presumption by performing and documenting a risk assessment using factors described in the Final Rules, but it is clear that HHS expects that most impermissible uses and disclosures of PHI will now be reportable events. This change will likely multiply the number of reported breaches to HHS.

Potential penalties currently in place have been retained, ranging from $100 to $50,000 per violation, capped at $1.5 million annually. While Business Associates and their subcontractors are now directly liable for HIPAA violations, Covered Entities may also be liable for Business Associate violations.

Deadlines for Compliance

The Final Rule is effective March 26, 2013. The compliance deadline for most provisions of the Final Rules is 180 days later, or **September 22, 2013**. A longer compliance period is provided for updates to existing business associate agreements and data use agreements. Those agreements do not need to be updated until September 22, 2014, unless they are modified or renewed prior to that date (see discussion under Security Rule).

[1] 78 Fed Reg. 5566.

Impact of the Final Rules on Business Associates

1. Expanded Definition of Business Associate

A "Business Associate"[2] is defined by HIPAA to be a person or entity who provides certain functions, activities and services to or on behalf of a covered entity involving the use or disclosure of PHI. The Final Rules clarify that persons or entities that "create, receive, maintain or transmit" PHI are considered Business Associates, expanding the definition to specifically include entities who merely store PHI. This definition may include technology providers and other vendors contracting with a Covered Entity.

Subcontractors of Business Associates are now themselves also considered to be Business Associates. Researchers may also be considered Business Associates if they perform a service for a Covered Entity[3], such as creating limited data sets and de-identifying PHI, even for their own research purposes.

2. Direct Liability for Security Rule/ Changes to Business Associate Agreement Requirements

The Final Rules implement the HITECH Act's provisions extending to Business Associates direct liability for compliance with the entire HIPAA Security Rule. This means that the administrative, physical and technical safeguard requirements; and policy, procedure and documentation requirements apply, as well as the requirement to have Business Associate Agreements in place with subcontractors which comply with the Security Rule (including requiring notification of breaches to the Business Associate). The Security Rule requires many documented policies and procedures to be in place and technical requirements to be performed (such as conducting a security risk analysis[4] and developing a formal mitigation plan, contingency plan, creating systems logs, monitoring user activity and possibly encrypting data.) Once in place, the organization must conduct and document regular workforce training on its risk management program.

HHS acknowledges the potential burden of compliance, particularly on smaller or less sophisticated organizations. To assist these organizations it their compliance efforts with the Security Rule, HHS provides educational materials and guidance documents on its website at http://www.hhs.gov/ocr/hipaa/administrative/securityrule.

3. Business Associate Agreements

The Final Rules require Business Associates to agree in business associate agreements to comply with the requirements of HIPAA. Business associate agreements must also require business associates to enter into business associate agreements with all subcontractors[5] who receive, create, or transmit PHI on their behalf. HHS

[2] Note that an organization may be a Business Associates even if only a part of its business is involved with HIPAA-covered functions (a "hybrid entity"). Those portions of an entity that engage in this function must comply with HIPAA, including the Final Rules.

[3] A "Covered Entity" under HIPAA is a health plan, health care clearing house and health care providers who transmit any health information in electronic form.

[4] After initial risk analysis, HHS also contemplates, as articulated on its website, www.hhs.gov/ocr/privacy/hipaa, that risk analysis be an "ongoing process, in which a covered entity regularly reviews its records to track access to e-PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to e-PHI."

[5] "Subcontractor" is defined as "a person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such business associate".

has released new model form business associate agreement language which complies with these requirements. The new model form can be found at http://www.hhs.gov/ocr/privacy/hipaa/undertsanding/coveredentities/contractprov.html.

The Final Rules provide that business associate agreements that were in effect prior to January 25, 2013 are deemed to be compliant with the prior regulations until September 22, 2014, unless they are amended during the year prior to that date. This allows additional time to amend existing agreements.

Business Associates should review their existing business associate agreements and subcontractor relationships to ensure, at a minimum, inclusion of provisions required by the Final Rules. Business Associates should expect the same review to be conducted by Covered Entities, which will likely result in requests for modification of existing business associate agreements with the Covered Entity. It is also appropriate to review and revise existing policies, procedures and other technical aspects of Business Associates' risk management programs and update workforce training.

4. Privacy Rule Requirements

Under the Final Rules, a Business Associate is directly liable for uses and disclosures of protected health information that are not in accord with the terms of its business associate agreement or the Privacy Rule. This includes failure to disclose PHI to the applicable Covered Entity, individual or individual's designee, as necessary to satisfy a Covered Entity's obligation with respect to an individual's request for an electronic copy of PHI; failure to make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended purpose of the use or disclosure or request; and failure to enter into business associate agreements with subcontractors that create or receive PHI on the Business Associate's behalf. Business Associates are also required to maintain an accounting of disclosures of PHI and provide PHI to HHS during an investigation or compliance review (which investigations and reviews are likely to be more numerous, given HHS's broadened enforcement authority and breach notification revisions discussed below).[6]

Note that HHS has not provided a definition of what constitutes "minimum necessary". However, the minimum necessary standard is a "condition of the permissibility of uses and disclosures of PHI". If an organization discloses more PHI than the minimum necessary to accomplish the intended purpose of the use or disclosure, it is not a permitted use or disclosure. While the Final Rules make this standard explicitly applicable to Business Associates, it also limits requests for PHI by Covered Entities and other Business Associates to this same standard. Business Associates may rely on these requests as requesting the minimum necessary for the disclosure.

The Final Rules explicitly make Covered Entities liable for their business associates' noncompliance. This may result in more requests by Covered Entities to conduct their own compliance audits of their Business Associates and request other revisions to contractual obligations contained in business associate agreements. Business Associates should expect requests by Covered Entities to amend business associate agreements to add/ supplement audit rights provisions as well as contain more robust indemnification. Similarly, Business Associates should consider adding these provisions to its subcontractor business associate agreements.

[6] However, business associates are not required to comply with all provisions of the Privacy Rules, including providing notice of privacy practices or designating a privacy official, unless a Covered Entity has delegated those obligations contractually to the business associate.

5. Modification to Breach Notification Requirements

HHS has imposed a tougher standard for determining when notification of security breaches is required. The Final Rules also change the definition of what constitutes a breach. Under the interim breach notification rule, a breach was defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted [by the Privacy Rule] which compromises the security or privacy of protected health information." The phrase "compromises the security or privacy of [PHI]" was defined to mean "pos[ing] *significant risk of financial, reputational, or other harm to the individual*" [emphasis added].

HHS notes in the Final Rules that this "risk of harm" standard may have been interpreted as setting a higher standard for breach reporting than what was intended by HHS. HHS goes on to clarify that under the Final Rules "an impermissible use or disclosure of protected health information[7] *is presumed to be a breach* unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been "compromised"[emphasis added]. Breach notification is required "in all situations except those in which the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised…." While HHS does not define the term "compromised", it requires a risk analysis to demonstrate a low probability of compromise which includes, at a minimum, the following factors:

i. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
ii. the unauthorized person(s) who used the PHI or to whom disclosure was made;
iii. whether the PHI was actually acquired or viewed;
iv. the extent to which the risk to the PHI has been mitigated.

Other factors may also be considered, where determined necessary.

Business Associates should document the risk analysis in each instance and retain such documentation to demonstrate that unreported incidents did not give rise to a reportable breach. Risk assessments are, by their nature, subject to individual judgment (which may differ from that of HHS). In recognition of this fact, HHS has noted in a comment that it would in the future issue additional guidance to assist organizations "in performing risk assessments with respect to frequently occurring scenarios."

HHS notes that a party has the discretion to disclose a breach without performing a risk assessment, but that the risk analysis is required in all cases where a party wishes not to disclose the breach. A party must still disclose the breach in the event the risk assessment fails to indicate a low probability that the PHI has been compromised. Business Associates must provide breach notifications to the applicable Covered Entity "without unreasonable delay and in no case later than 60 days from discovery of the breach". Notice must include the identity of the affected individuals to the extent possible. Business Associates are required to notify the applicable Covered Entity of the breach of unsecured PHI so that the Covered Entity can notify affected individuals (and HHS). Business

[7] Note, as set forth in the Breach Notification Rule, breach notification applies to unauthorized uses and disclosures of "unsecured protected health information". The Final Rule retains this concept. Accordingly, no breach notification will be required if the PHI is encrypted in conformity with HHS guidance.

Associates' subcontractors are required to provide notices to the Business Associate who in turn provides notice to the Covered Entity.

6. Prohibition on Sale of PHI

Consistent with the HITECH Act, the Final Rules prohibit the sale of PHI unless the individual has authorized it. A "sale" is made if the Business Associate receives remuneration, financial or otherwise, in exchange for PHI.[8] Remuneration is not limited to monetary payments, but includes in-kind benefits. The Final Rules contain certain narrow exceptions to the definition of "sale", including certain disclosures where the remuneration is a reasonable, cost based fee to cover the cost of preparing and transmitting the PHI. Fees charged to create a profit from the disclosure are not permitted.

Disclosures of limited data sets (a form of PHI[9] with certain identifiers removed in accordance with HIPAA requirements) for remuneration under existing data use agreements (in effect prior to 1/25/13) may continue until the earlier of September 22, 2014 or the next renewal or modification of such agreements. After that date, the restrictions in the Final Rules apply.

Disclosures of PHI which has been de-identified in accordance with the Privacy Rule[10] requirements are not subject to the remuneration prohibition, since this information is not considered to be PHI.

7. Limitations on use of PHI for Paid Marketing

The Privacy Rule requires Covered Entities to obtain authorization from individuals before using or disclosing PHI to market a product or service to them. Prior to the Final Rules, no authorization was required for communications involving treatment and healthcare operations. This is no longer the case under the Final Rules. Subject to some exceptions, authorizations must be obtained from individuals for use of PHI to make communications relating to treatment and healthcare operations if the Covered Entity (or its Business Associate) received financial remuneration from a third party whose product or service is being promoted.

8. Compliance Reviews and Enforcement

HHS has expanded enforcement authority and under the Final Rules is required to conduct compliance reviews. In addition, HHS is required to investigate complaints if it suspects willful neglect. Business Associates and their subcontractors will be subject to these compliance reviews and investigations. As part of these compliance reviews, HHS will request and review of Business Associates' HIPAA policies and procedures. For this reason, it is advisable for Business Associates to review and update policies to conform to the Final Rules and cause its subcontractors to do so as well.

---

[8] HHS defines "sale" of PHI to mean "a disclosure of protected health information by a covered entity or a business associate, if applicable, where the covered entity or business associate directly or indirectly receives remuneration from or on behalf of the recipient of the protected health information in exchange for the protected health information."

[9] HHS notes that it does not exempt disclosure of limited data sets from the rule provisions, as it does for de-identified data, because limited data sets "are still protected health information".

[10] See Privacy Rule at §164.514(b)-(d).

Note also that HHS is no longer required to (but may, in its discretion) attempt to resolve compliance issues informally, but may move directly to assessing penalties.

Action Steps for Business Associates to Consider

In advance of the compliance date for the Final Rules, Business Associates should consider the following action items:

- Update form business associate agreements to address changes contained in the Final Rules and to address the enhanced risk profile for Business Associates;
- Require all new subcontractors who may be provided access to PHI to execute the updated business associate agreement;
- Review existing subcontractor arrangements and bring these arrangements up to date, either with execution of new documents or amendments to existing business associate agreements;
- Perform a compliance review of existing policies and procedures and technical requirements and implement appropriate revisions. Consider using the HHS HIPAA Audit Protocol for your own compliance assessment, which can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html. Also consider consulting with counsel concerning establishing privilege for compliance review activities and results.
- Review any agreements relating to the sale of PHI or use of PHI for marketing and amend as appropriate;
- Be prepared to respond to requests by Covered Entities for modification of business associate agreements (which may include enhanced indemnification provisions relating to business associate and subcontractor acts and omissions);
- Provide workforce training to staff who may have access to PHI on the Final Rules and policy changes;
- Consider encrypting PHI in accordance with the Privacy Rule to lessen risks associated with inadvertent disclosures (see HHS guidance at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/de-identification/guidance.html);
- Correct and mitigate violations immediately. If violations occur prior to the compliance date for the Final Rules, Business Associates would be well served to perform risk assessments which comply with the Final Rules as well as applicable standards.