Legal Insight

K&L GATES

www.klgates.com

February 25, 2013

Practice Group:

Health Care

HIPAA's New Rules: Expanding Scope, Clarifying Uncertainties, and Reinforcing Fundamentals

By Patricia C. Shea

On January 25, 2013, the Secretary for the United States Department of Health and Human Services, Office for Civil Rights (the "Department") officially published the long-awaited final regulations (the "Final Rule") implementing extensive and sweeping changes to the regulations for the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Final Rule increases compliance obligations for covered entities and business associates regarding when, how, why, and in some cases "if" they may receive, maintain, transmit, create, use or disclose the health information HIPAA protects ("protected health information"). Quite simply, the Final Rule significantly affects **all** covered entities and business associates.

This is the first alert in a series that discusses significant changes to HIPAA compliance obligations. In addition to providing key compliance dates and a brief background about the Final Rule, this alert also offers insight into the expanded definition of "business associate" and the new requirements for business associate agreements.

Future alerts in this series will address:

- the modified requirements for analyzing potential breaches of unsecured protected health information;
- new requirements for notices of privacy practices;
- stricter requirements for marketing and sale of protected health information;
- modifications to access rights to information by individuals;
- enforcement; and
- implications for research.

Covered entities and business associates should consult with their legal counsel to determine the extent of the impact the Final Rule has with respect to them.

Important Dates

Perhaps the best news in the Final Rule is its effective and compliance dates. The final rule is **effective on March 26, 2013**, but compliance with the new provisions will not be enforced until **September 23, 2013**.[1] The Final Rule was officially published on January 25, 2013 so entities have **approximately 8 months to comply**. That is the good news. The bad news is that entities **only** have 8 months to get their HIPAA houses in order and to implement the changes.

[1] *See* 78 Fed. Reg. 5566, 5669 (Jan. 25, 2013) (hereinafter the "Final Rule"). The Final Rule also "make[s] clear to the industry our expectation that going forward we will provide a 180-day compliance date for future modifications to the HIPAA Rules." *Id.; see also id.* at 5689 (to be codified at 45 CFR § 160.105).

HIPPA's New Rules: Expanding Scope, Clarifying Uncertainties, and Reinforcing Fundamentals

Compliance efforts should begin **immediately**. CEOs, CFOs, legal counsel, and Privacy and Security Officers should be assigning responsibility for reviewing and understanding the modified compliance requirements and developing a project plan to assess and implement appropriately. This is not a simple task. Think broadly and involve workforce members from all levels and functions of the organization who may have access to or responsibility for the individually identifiable health information HIPAA protects ("protected health information" or "PHI").

Setting the Stage: How it all Began

Although HIPAA became law in 1996, the associated regulations came years later in stages.

Beginning in 2003, most entities subject to HIPAA (such as health care providers and health plans and collectively called "covered entities") were required to comply with HIPAA's implementing regulations governing the privacy of protected health information. These regulations, known as the "Privacy Rule," protect the use and disclosure of individually identifiable health information held by covered entities, and they specify rights individuals have with respect to their protected health information.

Beginning in 2005, covered entities were also required to comply with regulations implementing safeguards for protected health information created, received, transmitted, or maintained in electronic form. These regulations are known as the "Security Rule."

In February 2009, HIPAA was significantly strengthened by the passage of the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), included as a part of the Affordable Care Act. Among other things, the HITECH Act:

- significantly increased the fines and penalties for noncompliance with any of HIPAA's regulations;
- made certain parts of the Security Rule directly applicable to entities that performed functions on behalf of covered entities requiring the use or disclosure of protected health information (called "business associates");
- made certain provisions of the Privacy Rule applicable to business associates; and
- required covered entities to notify individuals of breaches of their protected health information in certain situations.

In August 2009, the Department issued interim regulations to implement the breach notification mandated by the HITECH Act (called the "Breach Notification Rule"). However, regulations governing most other aspects of the HITECH Act were not addressed.

In July 2010, the Department issued a notice of proposed rulemaking that addressed the bulk of the remaining HITECH Act mandates and provided a 60-day comment period. The notice of proposed rulemaking gave us a glimpse into how the Department might modify existing regulations to strengthen protections surrounding health information.

The Final Rule now implements the bulk of what the notice of proposed rulemaking included as well as some other changes to the Privacy, Security and Breach Notification Rules that the Department deemed necessary to strengthen protection and control for individuals regarding their protected health information. It makes some significant changes.

HIPPA's New Rules: Expanding Scope, Clarifying Uncertainties, and Reinforcing Fundamentals

Business Associates: A New Definition, New Requirements, and New Risks

Perhaps one of the most widely anticipated and publicized changes proposed in the notice of proposed rulemaking was the change to the definition of business associate.

BEFORE THE FINAL RULE: The Privacy Rule defined "business associate" as a person (or entity) who performs a function on behalf of a covered entity that requires the use or disclosure of protected health information.[2] Covered entities (i.e., health care providers, health care clearinghouses, and health plans) must have contracts with their business associates (called "business associate agreements") whereby business associates agree, among other things, not to use or disclose the protected health information inappropriately and to safeguard it from unauthorized acquisition.[3] In the event a business associate subcontracted a task that also required the subcontractor to use or disclose protected health information, the business associate had to obtain satisfactory assurances from, or otherwise ensure that, the subcontractor would likewise safeguard the information, but the business associate did not have to execute a business associate agreement with the subcontractor. Neither business associates nor their subcontractors, however, were directly subject to HIPAA.

In 2009, the HITECH Act changed these rules in a couple of significant ways. First, the HITECH Act made business associates subject to certain HIPAA requirements.[4] Specifically, the HITECH Act required business associates to comply with most of the Security Rule as well as some Privacy Rule requirements. Second, the HITECH Act made business associates liable for violations of those requirements.[5] Third, the HITECH Act significantly increased the civil and criminal penalties for violations.[6]

The Final Rule clarified how the HITECH Act requirements would be implemented and made other changes to address concerns the Department had regarding protected health information.

First, the Final Rule expands the definition of business associate to include a "subcontractor that creates, receives, maintains or transmits protected health information on behalf of the business associate."[7] As a result, any recipient of a delegated task that involves the creation, receipt, maintenance or transmission of protected health information is a business associate regardless of whether a covered entity or other business associate delegated the task. Accordingly, hereinafter references to "business associates" include persons and entities not previously included in the definition of "business associate" but who must create, receive, transmit or maintain protected health information to perform a permitted task that has been delegated to them. Defining "business associate" in this manner significantly expands the Department's authority over a group of people and entities that previously had no direct HIPAA obligations.

Second, the Final Rule requires that any person or entity that meets the definition of "business associate" execute a business associate agreement. If the task involving the protected health information is delegated by the covered entity, the covered entity must be a party to the business

[2] *See* 45 CFR 160.103.
[3] *Id.* at 164.308(b), 164.504(e)(1).
[4] *See* 42 U.S.C. §§ 17931(a), 17934(a).
[5] *See id.* at §§ 17931(b), 17934(c).
[6] *See id.* at §§ 1320d-5, 1320d-6.
[7] Final Rule at 5688 (to be codified at 45 CFR 160.103) (emphasis added). Other entities expressly included within the definition are Health Information Gateways, e-prescribing gateways, or such other person that "provides data transmission services with respect to protected health information and that requires access to such information on a routine basis." *Id.* The definition now also expressly recognizes that patient safety activities as defined at 42 CFR 3.20 fall within the types of activities that business associates would perform on behalf of a covered entity. *Id.*

associate agreement. If the task involving the protected health information is delegated by a business associate, the covered entity is not required to be a party to the business associate agreement. In that case, the business associate delegating the task and the business associate receiving the task must execute the business associate agreement.[8] Business associates who further delegate tasks involving the use or disclosure of protected health information must likewise execute business associate agreements.[9] As a result, many entities not previously subject to HIPAA will be required to execute business associate agreements and to meet the HIPAA requirements that apply directly to business associates. In addition, new business associates will incur liability for civil and criminal penalties for violating those requirements.

Third, although the HITECH Act specified the Security Rule provisions that would be applicable to business associates, it left some uncertainty as to the other HIPAA requirements that would apply directly to business associates. In response, the Department specified that business associates are directly liable under the HIPAA Rules for the following:

- Impermissible uses or disclosures of protected health information;
- Failure to provide breach notification to the covered entity;
- Failure to provide access to a copy of electronic protected health information either to the covered entity, the individual, or the individual's designee (as specified in the business associate agreement);
- Failure to disclose protected health information where required by the Department to investigate or determine the business associate's compliance with HIPAA Rules; and
- Failure to provide an accounting of disclosures.[10]

The Final Rule further explains that business associates must limit any permissible use or disclosure of protected health information to the minimum necessary amount to achieve a permitted purpose. The Department views "the minimum necessary standard [as] a condition of the permissibility of many uses and disclosures of protected health information."[11] Consequently, a use or disclosure of protected health information for which the requisite "minimum necessary" amount of protected health information has not been identified or that exceeds the minimum necessary would be impermissible under HIPAA. Business associates must make this assessment for themselves although they may "reasonably rely" on requests from other business associates or covered entities as requesting the minimum necessary for disclosure.[12]

In addition to expanding the definition of business associate, the Final Rule also made modifications to the requirements for the business associate agreements.

[8] *See id.* at 5694, 5698 (to be codified at 45 CFR 164.314(a)(2)(iii)) and 164.504(e)(5)).
[9] *See id.; see also id.* at 5694 (to be codified at 45 CFR 164.308(b)(2).
[10] *See id.* at 5598 - 5599.
[11] *See id.* at 5599. The HITECH Act defines "minimum necessary" as a limited data set. 42 U.S.C. § 17935(b)(1). A "limited data set" is protected health information in which almost all individual identifiers have been removed. *See* 45 CFR 164.514(e)(1). The Department plans to provide additional guidance on the minimum necessary standard. *See* Final Rule at *id.*
[12] *See id.*

HIPPA's New Rules: Expanding Scope, Clarifying Uncertainties, and Reinforcing Fundamentals

BEFORE THE FINAL RULE: Both the Privacy and Security Rules required that covered entities execute "business associate agreements" and specified the requirements for those agreements, including identifying permissible uses and disclosures of information. A covered entity could not disclose protected health information to a business associate without first executing this agreement. Most covered entities and business associates (as previously defined) had standard forms of business associate agreements.

The Final Rule specifies a number of changes to the content of business associate agreements to reflect changes required by the HITECH Act and to "reflect the Department's new regulatory authority with respect to business associates …"[13] These changes include:

- Eliminating the requirement to notify the Secretary in cases where there is a violation of business associate agreement when termination is infeasible;[14]
- Requiring all business associates to comply with the minimum necessary standard;[15]
- Requiring all business associates to comply with the obligations to safeguard electronic protected health information; report breaches of unsecured protected health information; and require subcontractors that create or receive protected health information to agree to the restrictions and conditions that apply to business associates with respect to protected health information;[16] and
- •If the business associate is performing an obligation of the covered entity, complying with all HIPAA requirements that apply to a covered entity performing such obligation.[17]

Health and Human Services has posted sample provisions that address these issues on its website.[18]

The Final Rule includes a grandfathering provision for business associate agreements in effect **prior** to January 25, 2013 (i.e., the publication date of the Final Rule) **if** the agreements (including any related service agreements) are not renewed or modified prior to the compliance date in the Final Rule (i.e., September 23, 2013).[19] The grandfathering provision provides business associates meeting these specifications an extra year (i.e., until September 22, 2014) to amend the business associate agreements to comply with the new requirements. The agreements will be deemed compliant with the Final Rule until either (i) the agreement is modified after the compliance date, or (ii) September 22, 2014, whichever occurs first.[20] The grandfathering provision applies only to the business associate agreement requirement and not to any other provision of the Final Rule.

---

[13] *See id.*; *see also* 42 U.S.C. §§ 17931(a), 17934(a).
[14] *See id.* at 5600.
[15] *See id.* at 5697 (to be codified at 45 CFR 164.502(b)(1)). "In short, each agreement in the business associate chain must be as stringent or more stringent as the agreement above with respect to the permissible uses and disclosures." *See id.* at 5601. Business associates must also respond to noncompliance on the part of their subcontractors in the same manner that a covered entity would be required to respond to a business associate's noncompliance. *See id.* at 5697 (to be codified at 45 CFR 164.504(e)(1)(iii)).
[16] *See id.* at 5697 (to be codified at 45 CFR 164.504(e)(1)(ii)).
[17] *See id.* at 5600 (to be codified at 45 CFR 164.504(e)(2)(ii)(H)).
[18] *See* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
[19] *See* Final Rule at 5702 (to be codified at 45 CFR 164.532(e)(1)). "Modification" should be viewed broadly to include any change to the business associate agreement or the related services agreement. In essence, any reason that would require a change to any part of the agreement would require the business associate agreement to be updated. *See id.* at 5603.
[20] *See id.* at 5702 (to be codified at 45 CFR 164.532(e)(2)).

HIPPA's New Rules: Expanding Scope, Clarifying Uncertainties, and Reinforcing Fundamentals

Putting it All Together

The Final Rule has materially changed the way covered entities and business associates will operate going forward with respect to HIPAA compliance. Privacy and Security Officers should be working with legal counsel to (1) identify policies and procedures that must be updated to reflect changed requirements and to address new ones; and (2) identify any existing subcontractors that qualify as business associates under the expanded definition and execute business associate agreements with them.

Author:

Patricia C. Shea
patricia.shea@klgates.com
+1.717.231.5870

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Diego San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C.

K&L Gates practices out of 47 fully integrated offices located in the United States, Asia, Australia, Europe, the Middle East and South America and represents leading global corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.

This publication is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.

©2013 K&L Gates LLP. All Rights Reserved.