MORRISON | FOERSTER

Morrison & Foerster Client Alert

June 5, 2013

Think You're Not Covered by HIPAA? Think Again.

By Andrew B. Serwin, Peter F. McLaughlin, and Melissa Crespo

The Department of Health and Human Services ("HHS") recently amended the Health Insurance Portability and Accountability Act ("HIPAA") regulations ("HIPAA Rules") in a way that may make many companies, particularly those in the technology sector, "Business Associates" and subject to many HIPAA requirements. This change, coupled with new enforcement powers for HHS, should make HIPAA a top-of-mind issue for many technology companies that previously did not have to worry about HIPAA's requirements or concluded that HIPAA did not apply to them. This is all the more true because HHS will begin enforcing the new standards in September 2013, and companies that are not compliant will face significant enforcement risk. As a result, companies need to be proactive in determining whether they are Business Associates, how they are going to manage the HIPAA-mandated Business Associate Agreements, and whether the subcontractors they engage are complying with the new standards.

BACKGROUND

HIPAA generally covers two types of entities—"Covered Entities" and "Business Associates"— and it governs the use of certain individually identifiable health information ("Protected Health Information" or "PHI") by imposing privacy, security, and breach reporting requirements, as well as restrictions on marketing activities involving PHI. When the original version of the HIPAA Rules was enacted, the definition of a Business Associate was more limited than it is in the final Rule. To understand the new scope of what a Business Associate is, it is helpful to understand what these terms originally meant.

Covered Entities are generally defined as health care providers that transmit PHI electronically, health plans (such as health insurers, HMOs, and company health plans), and health care clearinghouses, which are essentially data intermediaries.[1] This focused definition has not changed under the final Rule, but the same cannot be said for the definition of Business Associates. In the past, there was a two-prong definition of a Business Associate, but the definition has changed in four key ways.

[1] 45 C.F.R. 160.103.

UNITED STATES

California
Tiffany Cheung (415) 268-6848
Rebekah Kaufman (415) 268-6148
Christine E. Lyon (650) 813-5770
David F. McDowell (213) 892-5383
James R. McGuire (415) 268-7013
Daniel F. Muto (858) 720-7959
Purvi G. Patel (213) 892-5296
Andrew Serwin (858) 720-5134
William L. Stern (415) 268-7637
Nancy R. Thomas (213) 892-5561

New York
Cindy Abramson (212) 336-4178
Melissa Crespo (212) 336-4354
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Peter McLaughlin (212) 336-4290
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian Waldmann Agarwal (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Virginia
Daniel P. Westman (703) 760-7795

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
L. Richard Fischer (202) 887-1566
D. Reed Freeman, Jr. (202) 887-6948
Julie O'Neill (202) 887-8764
Obrea O. Poindexter (202) 887-8741
Cynthia J. Rich (202) 778-1652
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

EUROPE

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364
Alja Poler De Zwart 32 2 340 7360

London
Ann Bevitt 44 20 7920 4041
Anthony Nagle 44 20 7920 4029
Caroline Stakim 44 20 7920 4055
David Varney 44 20 7920 4058

ASIA

Beijing
Gabriel Bloch 86 10 5909 3367
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Hong Kong
Gordon A. Milner 852 2585 0808

Tokyo
Daniel P. Levison 81 3 3214 6717
Gabriel E. Meister 81 3 3214 6748
Jay Ponazecki 81 3 3214 6562
Toshihiro So 81 3 3214 6568
Yukihiro Terazawa 81 3 3214 6585

First, Section (1)(i) of the old definition included a person who, on behalf of a covered entity or an organized health care arrangement (in certain circumstances) performed, or assisted in the performance of "a function or activity involving the use or disclosure of individually identifiable health information," including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing, or any other function or activity regulated by HIPAA.

Under the final Rule, Section (1)(i) was expanded to include any person that, on behalf of a covered entity, "creates, receives, maintains, or transmits protected health information for a function or activity regulated by [HIPAA] ", including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, certain patient safety activities, billing, benefit management, practice management, and repricing.[2]

In other words, the key language defining the activities of such third-party providers is significantly broader. In the past, technology and service providers could argue that their offering did not involve "the use or disclosure of individually identifiable health information." The language of the current definition is intentionally broad to encompass almost all entities that have any responsibility for "creat[ing], receiv[ing], maintain[ing], or transmit[ting] protected health information."[3]

Second, Section (3)(i) of the definition of Business Associate was changed, and HHS amended the Rule to state that a Business Associate also includes Health Information Organizations, E-prescribing Gateways, or another person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.[4]

Third, Section (3)(ii) further expanded the definition of a Business Associate to include people that offer personal health records to one or more individuals on behalf of a covered entity.[5]

Fourth, and as significant as the first modification, the definition of a Business Associate now includes subcontractors that create, receive, maintain, or transmit PHI on behalf of a Business Associate. The factors that determine whether a primary contractor is a Business Associate also apply to the determination of whether a subcontractor is a Business Associate. The goal of this change, in the view of HHS, was to prevent a lapse in coverage regarding privacy and security of PHI once a subcontractor is enlisted to assist a primary Business Associate. Importantly, according to HHS, this also creates downstream liability for subcontractors that did not exist before.

These changes are an expansion of the definition of a Business Associate, particularly for companies that provide technology support for Covered Entities, and these changes drew a significant number of comments, as well as some guidance from HHS about how it may interpret these standards. The first issue that drew attention was what it meant to access PHI "on a routine basis," as many technology providers could claim that they are not expected to access PHI on anything but an infrequent basis. HHS considered such comments but maintained in the final rule that even though a technology provider might never intend to access PHI, if it is possible for the provider to do so, then that provider will likely be considered a Business Associate. HHS did state that where a company acts as a "mere conduit"—such as a

[2] 45 C.F.R. 160.103(1)(i).

[3] 45 C,F.R. § 160.103(1)(i).

[4] 45 C,F.R. § 160.103(3)(i).

[5] 45 C,F.R. § 160.103(3)(ii).

telecommunications company, ISP, or courier service—it is not a Business Associate. HHS also emphasized that this exception is narrow so that, for example, a records storage provider would be considered a Business Associate because it "maintains" PHI. The analysis of who is a Business Associate versus who is not is a "fact-specific" analysis based upon the nature of the services provided and the extent to which the company needs access to PHI to provide services to the Covered Entity. It is important to note, though, that there is no knowledge component to the determination; that is, a company may be found to be a Business Associate without even knowing it.

For technology companies, this creates some ambiguity because, while HHS did identify ISPs as generally being conduits, other companies that provide data support or storage may now fall within the expanded definition of a Business Associate. According to HHS, this is true even if the company that is offering storage or other support does not *actually view* the PHI. As a result, a software company that hosts software or data containing PHI on its own server, or accesses PHI when troubleshooting the software function, is considered a Business Associate. The expanded regulation also affects data storage providers, including cloud storage providers, to the extent they store PHI on behalf of a Covered Entity or Business Associate, unless the cloud storage provider falls within the narrow "conduit" exception.

HHS also offered guidance regarding the personal health record (PHR) issue, which is relevant for service providers as well as mobile app developers providing PHR services. While there may be PHR vendors that do not fall within HIPAA because they are offering PHRs to a person directly, and not on behalf of a Covered Entity, PHR vendors can be Business Associates according to HHS if they merely have access to PHI from a Covered Entity. This is true even if the PHR vendor does not actually access the information. Thus, an app developer that enables a consumer and the consumer's health provider to upload data needs to consider HIPAA if the developer pulls from the app seemingly innocuous information about the consumer.

These changes, coupled with the guidance HHS offered, illustrate that the Business Associate definition is expanding, particularly for companies that provide technical and operational support for Covered Entities. The fact-specific nature of the analysis makes drawing firm conclusions difficult at times, which means that companies that are in this space must be careful to avoid the pitfalls of the new definition.

REQUIREMENTS FOR BUSINESS ASSOCIATES

The statutory changes that resulted in amendments to the HIPAA Rules extend to Business Associates direct statutory and regulatory obligations that were previously only imposed on Covered Entities. This means that the Security Rule, the Breach Notification Rule, and certain provisions of the Privacy Rule now apply directly to Business Associates, with the potential for enforcement by HHS directly against the Business Associate. As a result, Business Associates are now required to conduct a risk analysis to assess the nature and volume of electronic PHI ("ePHI") and the risks of unauthorized use or disclosure of PHI. They must implement administrative, technical, and physical safeguards appropriate to the risks and vulnerabilities identified in the risk analysis. While many technology and service providers

probably have internal data security programs, those will need to be reviewed and updated to reflect the specific requirements of the HIPAA Rules.

BUSINESS ASSOCIATE AGREEMENTS

Prior to the amended rules, Business Associates were required to "[e]nsure that any agents, including a subcontractor, to whom it provides protected health information . . . agrees to the same restrictions and conditions that apply to such Business Associate with respect to such information."[6] The modified HIPAA Rules now require a Business Associate to obtain satisfactory assurances from a subcontractor that the subcontractor will properly safeguard information if the subcontractor is to create, receive, maintain, or transmit ePHI on behalf of the Business Associate. This requires that a Business Associate enter into a Business Associate agreement with its subcontractors and directly places the burden of supervising subcontractors on the Business Associate, rather than the Covered Entity. The obligation of a Business Associate to obtain satisfactory assurances from its subcontractors passes through to the subcontractor and any of its subcontractors, and in light of this Business Associates should consider what other steps they may need to take to protect themselves.

Failure to enter into a Business Associate agreement where one is required violates HIPAA and is punishable by civil and criminal penalties. Each day of noncompliance may be a separate HIPAA violation with civil penalties of up to $50,000 per violation and up to $1,500,000 per identical violation per year.

CHANGES TO ENFORCEMENT FOR BUSINESS ASSOCIATES

In the past, HHS did not have direct enforcement authority over Business Associates, in the absence of certain conditions being met. Now, HIPAA has been amended to give HHS direct enforcement authority over Business Associates. Moreover, as noted above, this creates liability for entities that may not be in direct contractual privity with the Covered Entity, given the commentary by HHS regarding downstream subcontractor liability.

PRACTICAL CONSIDERATIONS

The revised HIPAA Rules became effective on March 26, 2013, and, subject to certain exceptions, require Covered Entities and Business Associates to comply with the updated regulations by September 23, 2013. In advance of the compliance date, the key things technology companies must do include:

- assessing whether they providing services to Covered Entities that place them in the expanded definition of a Business Associate;
- determining whether they are a subcontractor to a company that may now be a Business Associate, as subcontractors of Business Associates are now also considered to be Business Associates;
- analyzing the new requirements for Business Associates to see if their existing policies and procedures meet the new HIPAA standards;
- ensuring that they are properly downstreaming any obligations to subcontractors; and
- considering whether there are terms in technology contracts that need to be reassessed in light of these changes.

While there are many other steps to be taken, these measures should provide some initial guidance about whether HIPAA

[6] 45 C.F.R. § 164.50(e)(ii)(D).

now impacts your company.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for nine straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law*," or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.