JONES WALKER

e*bulletin

HEALTH CARE

February 2013 Vol. 17 healthcare@joneswalker.com

HHS ISSUES LONG-AWAITED HIPAA OMNIBUS FINAL RULE – PART I

After much anticipation, on Thursday, January 17, 2013, the Department of Health and Human Services ("HHS"), Office of Civil Rights ("OCR") released the long-awaited Health Insurance Portability and Accountability Act of 1996 ("HIPAA") final rule.[1] The omnibus rule titled, "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules" ("Rule" or "Final Rule"), makes significant changes to HIPAA's Privacy, Security and Enforcement rules in accordance with the Health Information Technology for Economic and Clinical Health ("HITECH") Act, as further described below.[2]

In a News Release, dated January 17, 2013 ("News Release"), OCR Director Leon Rodriguez stated that the Final Rule " . . . marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented. These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability of my office to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."

In addition to strengthening the privacy and security protections of individual health information, HHS states that the Final Rule is designed to increase flexibility for, and decrease burdens on, regulated entities. HHS notes that the changes contained therein are consistent with, and arise in part from, HHS' obligations under Executive Order 13563 to conduct a retrospective review of its existing regulations to identify ways to reduce costs and increase flexibility under the HIPAA Rules.[3]

Prior Rules

The Final Rule, the pre-publication version of which is 563 pages long, finalizes numerous modifications to the HIPAA Rules which have been contained in four separate rules published by HHS since 2009. HHS indicates that the four rules have been combined to make up the Final Rule in order to reduce the impact and number of times certain compliance activities need to be undertaken by the regulated entities. Of the four rules, two of the rules are interim final rules while the other two rules are proposed rules.

---

[1] The Final Rule was published in the Federal Register on Friday, January 25, 2013. 78 Fed. Reg. 5566 (Jan. 25, 2013).

[2] The HIPAA Privacy and Security Rule, 45 C.F.R. Part 160 and Part 164, and the HIPAA Enforcement Rule, 45 C.F.R. Part 160, may collectively be referred to herein as the "HIPAA Rules."

[3] Please see our June 2012 E*Bulletin entitled "CMS Releases Final Rules for Health Care Providers" for a discussion of Executive Order 13563, Medicare regulatory reform, and certain revisions to the Medicare Conditions of Participation.

First, on August 24, 2009, HHS published in Interim Final Rule[4] setting forth breach notification provisions, which became effective September 23, 2009 ("Interim Breach Notification Rule"). HHS then published an Interim Final Rule[5] on October 30, 2009, which incorporated the HITECH Act's increased and tiered civil money penalty structure, which became effective on November 30, 2009 ("Interim Enforcement Rule"). Next, on July 14, 2010, HHS published a proposed rule[6] to implement certain privacy, security, and enforcement provisions of the HITECH Act ("2010 Proposed Rule"). Finally, on October 7, 2009, HHS published a proposed rule,[7] which HHS states is designed to strengthen the privacy protections for genetic information under the HIPAA Privacy Rule by implementing the protections for genetic information required by the Genetic Information Nondiscrimination Act of 2008 ("GINA") and would prohibit most health plans from using or disclosing genetic information for underwriting purposes ("GINA Proposed Rule"). As discussed in greater detail below, the Final Rule incorporates, modifies, and/or supplants the foregoing proposed and interim final rules.

We wish to note that *not* addressed in the Final Rule are the accounting for disclosures requirements, which were the subject of a separate proposed rule published by HHS on May 31, 2011.[8] HHS notes that this proposed rule is intended to implement the statutory requirement under the HITECH Act to require covered entities and business associates to account for disclosures of protected health information to carry out treatment, payment, and health care operations if such disclosures are through an electronic health record. HHS states that the accounting for disclosures will be the subject of future rulemaking.

Effective and Compliance Dates

The Final Rule is effective March 26, 2013 ("Effective Date"). Covered Entities ("CEs") and Business Associates ("BAs") have 180 days after the Effective Date, or until September 23, 2013 ("Compliance Date"), to comply with most of the provisions of the Final Rule, including, without limitation, the breach notification provisions. However, certain provisions of the Final Rule have different compliance dates. For example, as discussed below, CEs and BAs may continue to operate under certain existing business associate agreements for up to one year beyond the Compliance Date, provided certain conditions are met. In addition, the Final Rule states that the 180-day compliance period does not apply to the

[4] 74 Fed. Reg. 42740. The Interim Breach Notification Rule is titled, "Breach Notification for Unsecured Protected Health Information."

[5] 74 Fed. Reg. 56123. The Interim Enforcement Rule is titled, "HIPAA Administrative Simplification: Enforcement."

[6] 75 Fed. Reg. 40868. The 2010 Proposed Rule is titled, "Modifications to the HIPAA Privacy, Security, and Enforcement Rules Under the Health Information Technology for Economic and Clinical Health Act."

[7] 74 Fed. Reg. 51698. The GINA Proposed Rule is titled, "HIPAA Administrative Simplification: Standards for Privacy of Individually Identifiable Health Information."

[8] 76 Fed. Reg. 31426. The Proposed Rule is titled, "HIPAA Privacy Rule Accounting of Disclosures Under the Health Information Technology for Economic and Clinical Health Act."

enforcement provisions that are contained in the Final Rule. Rather, compliance with the Final Rule's enforcement provisions is as of the Effective Date.

The Final Rule also states that, as a general matter, with respect to new or modified HIPAA standards or implementation specifications, CEs and BAs will have 180 days from the effective date of any such new or modified standards or specifications to comply therewith. If any future new or modified standards or specifications require a longer compliance period, HHS will expressly specify the longer compliance period in the regulatory text.

Brief Overview

This E*Bulletin is meant to provide a brief overview of certain significant provisions of the Final Rule and focuses on the following provisions:

- provisions covering BAs, including, without limitation, the direct liability of BAs and subcontractors of BAs for compliance with certain provisions of the HIPAA Privacy Rule and the HIPAA Security Rule, and changes to requirements for Business Associate Agreements ("BAAs");

- breach notification provisions, which supplant many of the provisions contained in the Interim Breach Notification Rule, and which, among other things, remove the "harm standard," and replace it with a four-part "objective" assessment designed to measure the extent to which protected health information ("PHI") may have been compromised; and

- enforcement provisions, which generally incorporate the provisions of the Interim Enforcement Rule, with certain modifications and additional guidance.

Certain of the Final Rule's provisions that are not addressed in this E*Bulletin, including, without limitation, provisions relating to marketing, fundraising, authorizations, research, the sale of PHI, modifications as a result of GINA, and the Notice of Privacy Practices, will be the subject of future E*Bulletins.

I. Business Associates & Business Associate Agreements

The Final Rule contains a number of changes to, and expands the definition of, "business associate" to include, without limitation, persons that provide certain data transmission services and certain subcontractors. The Final Rule also imposes direct liability on BAs and adds provisions that must be contained in BAAs.

Business Associate Definition. In its Final Rule, HHS expands the definition of "business associate" to add patient safety activities to the list of functions and activities undertaken on behalf of a CE that give rise to a BA relationship. HHS states that this was done to more clearly align the HIPAA Rules with the Patient Safety Rules (42 C.F.R. §§3.10, et seq.).[9] In

[9] HHS notes that "PSQIA [the Patient Safety and Quality Improvement Act of 2005], at 42 U.S.C. 299b-22(i)(1), provides that Patient Safety Organizations (PSOs) must be treated as business associates when applying the Privacy Rule. PSQIA provides for

addition, the Rule expands the definition of BA to include a person who offers personal health records to one or more individuals on behalf of a CE, as well as a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a CE and that requires access on a routine basis to such PHI.

Data Transmission Services. As noted above, the new definition of BA includes persons that provide data transmission services with respect to PHI to a CE and that require "routine access" to such PHI. In the Final Rule, HHS distinguishes between providers of data transmission services that would be considered BAs versus those that would be mere "conduits." To determine whether such providers would be BAs or conduits, HHS notes that the analysis must focus on whether the entities providing data transmission services will have "routine access" to PHI. This determination, according to HHS, will be fact specific, based on the nature of the services provided and the extent to which the entity needs access to PHI to perform the services for the CE. HHS explains that the exception for mere "conduits" is narrow and is intended "to exclude only those entities providing mere courier services," such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers providing mere data transmission services. A conduit, HHS explains, transports information but does not access it other than on a random or infrequent basis, as necessary to perform the transportation service or as required by other law.

Subcontractors. A broad expansion of the definition of BA under the Final Rule is the inclusion of subcontractors who perform services for BAs and require access to PHI. These subcontractors are now, in and of themselves, considered to be BAs. This expansion was proposed in the July 2010 Proposed Rule, where HHS proposed to modify the definition of BA to include persons that perform functions for or provide services to a BA other than in the capacity as a member of the BA's workforce, to the extent that they require access to PHI. HHS notes that the intent of the proposed expansion to include subcontractors was to avoid having privacy and security protections for PHI lapse because a function is performed by an entity that is a subcontractor of a CE, rather than an entity that has a direct relationship with a CE. The Final Rule adopts this proposed expansion and applies business associate provisions to "downstream entities" that work at the direction of or on behalf of a BA and receive, access, maintain, and/or disclose PHI.

Accordingly, the Final Rule defines the term "subcontractor" as a person to whom a BA delegates a function, activity, or service, other than in the capacity of a member of the workforce of such BA. HHS states that a subcontractor will then be considered to be a BA if the function, activity, or service provided by the BA involves the creation, receipt, maintenance, or transmission of PHI. (Subcontractors who are BAs may be referred to herein as "BA subcontractors.") HHS notes in the Final Rule that a BA relationship is established by virtue of the services the BA provides and whether they involve PHI, and that such relationships can exist regardless of whether the parties enter into a BAA or other written contract.

Thus, the definition of BA now includes "a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate." This means that, as described by HHS and as further discussed below, "downstream entities" that work at the direction of or on behalf of a BA and handle PHI are also required to comply with

---

the establishment of PSOs to receive reports of patient safety events or concerns from providers and provide analyses of events to reporting providers. A reporting provider may be a HIPAA covered entity and, thus, information reported to a PSO may include protected health information that the PSO may analyze on behalf of the covered provider. The analysis of such information is a patient safety activity for purposes of PSQIA and the Patient Safety Rule, 42 CFR 3.10, *et seq*."

the applicable Privacy and Security Rule provisions in the same manner as the BA (and likewise would incur liability for acts of noncompliance).

In addition, in addressing commenters' concerns that the extension of the definition of BAs to subcontractors will, among other things, result in CEs prohibiting BAs from engaging subcontractors to perform functions or services that require access to PHI, HHS states that it believes that the extension will actually alleviate CEs' concerns that PHI would not be adequately protected if provided to subcontractors. HHS notes further that, just as CEs have had to obtain satisfactory assurances from BAs that the BAs will appropriately safeguard any PHI in their possession, BAs must now obtain such assurances from its BA subcontractors "and so on, no matter how far 'down the chain' the information flows." HHS makes clear that the CE is neither required to contract directly with, nor obtain satisfactory assurances from, the BA subcontractor. These are the obligations of the BA. This is the case with respect to BAs and BA subcontractors. Thus, every entity in the chain who is a BA or BA subcontractor must comply with requirements imposed on BAs, and may be subject to civil monetary penalties (as discussed hereinbelow) for failure to do so.

Finally, HHS notes that §§164.308(b)(2) and 164.502(e)(1)(ii) of the HIPAA Rules that have described certain circumstances in which a CE is not required to enter into a business associate contract or other arrangement with the recipient of the PHI, such as when a CE discloses PHI to a health care provider concerning the treatment of an individual, are relocated under the Final Rule to the definition of BA. HHS indicates that these exceptions have been relocated to the definition of BA to make clear that HHS does not consider the recipients of the PHI in these situations to be BAs.

Direct Liability of Business Associates

According to the News Release, "some of the largest breaches reported to HHS have involved business associates." Perhaps with this in mind, HHS makes clear in the Final Rule that BAs are now directly liable for violations of certain HIPAA Privacy and Security Rules.

Security Rule. Under the Final Rule, BAs are directly liable for compliance with the Security Rule. Accordingly, BAs must comply with the Security Rule in the same manner as CEs, including with respect to the Security Rule's administrative, physical, and technical safeguards requirements, as well as the Security Rule's policies and procedures, and documentation requirements.

In response to concerns raised regarding the cost of complying with these provisions, HHS notes that BAs and BA subcontractors should already have in place security practices that comply with the Security Rule (or, with "modest improvements" will comply with the Security Rule) by virtue of the fact that CEs have been required to enter into BAAs that require BAs to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic PHI ("ePHI") that they create, receive, maintain, or transmit on behalf of the CE. BAs have also been required, according to HHS, to ensure that any agents, including subcontractors, to whom they provide such information agree to implement reasonable and appropriate safeguards to protect it. Moreover, HHS notes that the requirements of the Security Rule were designed to be "technology neutral and scalable to all different sizes" of CEs and BAs, and thus CEs and BAs have the flexibility to choose security measures appropriate for

their size, resources, and the nature of the security risks they face, enabling them to reasonably implement any given Security Rule standard.

In addition, HHS notes that it made technical revisions to §164.306(e) in the Final Rule to more clearly indicate that CEs and BAs must review and modify security measures as needed to ensure the continued provision of reasonable and appropriate protection of ePHI, and that they update documentation of such security measures accordingly.

Privacy Rule. Unlike with respect to the Security Rule, under the Final Rule, BAs are directly liable for complying with certain, but not all, requirements of the Privacy Rule. Accordingly, in response to comments requesting clarification on with which HIPAA provisions a BA is directly liable for compliance, HHS states that BAs are directly liable under the HIPAA Rules for (1) impermissible uses and disclosures of PHI; (2) a failure to provide breach notification to the CE; (3) a failure to provide access to a copy of electronic PHI to either the CE, the individual, or the individual's designee (whichever is specified in the BAA); (4) a failure to disclose PHI where required by the Secretary of HHS ("Secretary") to investigate or determine the BA's compliance with the HIPAA Rules; (5) a failure to provide an accounting of disclosures;[10] and (6) a failure to comply with the requirements of the Security Rule. As discussed below, BAs are also liable for, among other things, a failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose, as well as a failure to enter into BAAs with its BA subcontractors. Further, HHS reminds entities that "[b]usiness associates remain contractually liable for other requirements of the business associate agreement."

HHS also notes that a BA's liability does not depend on (1) whether or not a BAA is in place; (2) the type of PHI that a BA creates, receives, maintains, or transmits on behalf of a CE or another BA; or (3) the type of entity performing the function or service (except to the extent the entity falls within one of the exceptions to the definition of BA).

As noted above, BAs are not required to comply with all requirements of the Privacy Rule. For example, BAs are not required to provide notices of privacy practices nor are they required to designate privacy officials. However, a CE may require, through its BAAs, that its BAs to comply with provisions of the Privacy Rule with which they are not otherwise required to comply. In such event, a BA's failure to comply with such provisions of a BAA would result in contractual liability.

Minimum Necessary. The Final Rule applies the "minimum necessary" standard directly to BAs. Thus, when BAs use, disclose, or request PHI from another CE, they must limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The Final Rule also makes clear that requests directed to another BA, in addition to those directed to another CE, must also be limited to the minimum necessary. As a result of this requirement, HHS notes that CEs and BAs that disclose PHI in response to a request from a BA are permitted to reasonably rely on the

[10] With respect to this requirement, HHS cites the Proposed Rule on Accounting of Disclosures, 76 Fed. Reg. 31426 (May 31, 2011), which is designed to implement the statutory requirement under the HITECH Act to require CEs and BAs to account for disclosures of PHI to carry out treatment, payment, and health care operations if such disclosures are through an electronic health record. As noted in the Proposed Rule, Section 13405(c) of the HITECH Act provides that the exemption at § 164.528(a)(1)(i) of the Privacy Rule for disclosures to carry out treatment, payment, and health care operations no longer applies to disclosures "through an electronic health record." As previously noted, HHS indicated that the Proposed Rule will be the subject of future rulemaking.

request as requesting only the minimum necessary with respect to the disclosure. HHS notes, however, that the manner in which the BA will apply the minimum necessary standard will vary based on the particular circumstances. In addition, HHS indicates that it is left to the parties to determine to what extent a BAA will include specific minimum necessary provisions that ensure a BA's uses and disclosures and requests for PHI are consistent with the CE's minimum necessary policies and procedures. HHS notes in the Final Rule that it expects to issue future guidance on the minimum necessary standard that will consider the specific questions posed by commenters with respect to BAs' application of the minimum necessary standard.

Business Associate Agreements

As a result of a number of comments HHS received regarding the necessity of BAAs, HHS makes clear that, despite a BA's direct liability for certain provisions of the HIPAA Privacy and Security Rules, a BAA is necessary. According to HHS, a BAA is necessary to clarify and limit, as appropriate, the permissible uses and disclosures by the BA, in light of the relationship between the parties and the activities or services being performed by the BA. The BAA is also necessary, HHS indicates, to ensure that the BA is contractually required to perform certain activities for which direct liability does not attach (such as the requirement to amend PHI). In addition, a BAA is, in HHS' view, an opportunity for the parties to clarify their respective responsibilities under the HIPAA rules, such as by establishing how the BA should handle a request for access to PHI that it directly receives from an individual. Finally, HHS notes that BAAs help to make BAs aware of their obligations and potential liabilities under the HIPAA Rules.

As noted above, a CE may disclose PHI to a BA if it obtains satisfactory assurances, in the form of written contract or information, from its BA that the BA will appropriately safeguard the PHI. The Final Rule includes a parallel provision that allows a BA to disclose PHI to a BA subcontractor, and to allow the BA subcontractor to create or receive PHI on its behalf, if the BA obtains similar satisfactory assurances that the BA subcontractor will appropriately safeguard the information. As also noted above, the CE is not required to obtain satisfactory assurances from the BA subcontractor. Rather, the BA is required to obtain such satisfactory assurances.

In addition, the Final Rule makes clear that the requirements for agreements between CEs and their BAs (set forth at 45 C.F.R. §164.504(e)(2)-(4)) also apply to agreements between BAs and BA subcontractors. That is, the requirements applicable to BAAs or other arrangements between a CE and a BA apply in the same manner to contracts or other arrangements between BAs and BA subcontractors. For example, HHS notes that a BA contract between a BA and a BA subcontractor would need to provide that the BA subcontractor report any security incident of which it becomes aware, including breaches of unsecured PHI to the BA. This would mean that if a breach of unsecured PHI occurs at or by a second tier BA subcontractor, the BA subcontractor must notify the BA subcontractor with which it contracts of the breach, which then must notify the BA which contracts with the CE of the breach, which then must notify the CE of the breach. The CE must then notify the affected individuals, the Secretary, and, if applicable, the media, of the breach, unless it has delegated such responsibilities to its BA under the BAA.

Further, HHS notes that the agreement between a BA and a BA subcontractor may not permit the BA subcontractor to use or disclose PHI in a manner that would not be permissible if done by the BA. Thus, HHS states that each agreement in the

BA chain must be as stringent or more stringent as the agreement above it with respect to the permissible uses and disclosures. For example, if a BAA between a CE and a BA subcontractor does not permit the BA subcontractor to de-identify PHI, then the BAA between the BA subcontractor and another downstream BA subcontractor (and the agreement between the BA subcontractor and another BA subcontractor) cannot permit the de-identification of PHI.

Certain other changes in the Final Rule that affect BAAs include, without limitation:

- removal of the requirement that CEs report to the Secretary of HHS when termination of a BAA is not feasible (such reporting has been required in the event a CE knew of a pattern of activity or practice of the BA that constituted a material breach or violation of the BA's obligation under a BAA, and the CE could not cure the breach or end the violation, or terminate the BAA);[11]

- requiring BAs who are aware of noncompliance by its BA subcontractor to respond to the situation in the same manner as a CE that is aware of noncompliance by its BA; and

- adding specific new provisions that are required in a BAA, including provisions stating that:

    - BAs must comply with the Security Rule with respect to ePHI;
    - BAs must report breaches of unsecured PHI to CEs;
    - BAs must ensure that any subcontractors that create or receive PHI on behalf of the BA agree to the same restrictions and conditions that apply to the BA with respect to such information; and
    - to the extent a BA carries out a CE's obligations, the BA must comply with the requirements of the Privacy Rule that apply to the CE in the performance of the obligations. (Note that the BA would be contractually liable for a violation of this requirement, but would not be directly liable unless the requirement were one with respect to which the Final Rule imposes direct liability on the BA.)

As previously discussed, compliance with many of the provisions of the Final Rule is September 23, 2013. However, the Final Rule allows CEs and BAs (and BAs and BA subcontractors) to continue to operate under certain existing contracts for *up to* one year beyond the Compliance Date *if*, prior to the publication date of the Final Rule (January 25, 2013), the CE or BA had an existing contract or other written arrangement with a BA or BA subcontractor, respectively, that complied with the prior provisions of the HIPAA Rules and such contract or arrangement is not renewed or modified between the Effective Date (March 26, 2013) and the Compliance Date (September 23, 2013). If this is the case, then HHS notes that the parties will have up to one year to modify their agreements to comply with the Final Rule. If however, during that one year, the parties renew or amend the otherwise "grandfathered" agreement, then such agreement will need to comply with the Final Rule at the time of the renewal or modification. Thus, CEs and BAs must comply with the Final Rule's requirements with respect to BAAs or contracts within one year of the Effective Date of the Rule, or when they

[11] In removing this requirement, HHS notes that "[i]n light of a business associate's direct liability for civil money penalties for certain violations of the business associate agreement and both a covered entity's and business associate's obligations under Subpart D [of Part 164] to report breaches of unsecured protected health information to the Secretary, we have other mechanisms through which we expect to learn of such breaches and misuses of protected health information by a business associate."

modify or renew their agreements, whichever is sooner. HHS notes that written evergreen contracts would also be eligible for the one-year extension but only if the contracts renewed automatically without any change in terms or other actions by the parties during such year.

Finally, on January 25, 2013, HHS published sample BAA provisions on its website to help CEs and BAs "more easily comply" with the requirements of the Final Rule. The website notes that, while these sample provisions are written for the purposes of the contract between a CE and its BA, the language may be adapted for purposes of the contract between a BA and its BA subcontractor. The website states, however, that the provisions are "only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules." In addition, the website notes that the sample language may be changed to more accurately reflect business arrangements between the parties. Further, it states that reliance on the sample provisions may not be sufficient for compliance with State law and "does not replace consultation with a lawyer or negotiations between the parties to the contract."

II. Breach Notification Provisions

Perhaps some of the most anticipated changes to the Final Rule are the changes to the breach notification provisions that are currently contained in the Interim Breach Notification Rule. The Final Rule, among other things, modifies the definition of "breach," contains a new breach assessment approach which, among other things, eliminates the "harm standard," and makes certain changes to notifications by BAs.

The Definition of Breach and Breach Assessments

The Interim Breach Notification Rule has defined the term "breach" to mean generally "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 the protected health information." The term "compromises the security or privacy of the protected health information" means "poses a significant risk of financial, reputational, or other harm to the individual" (the "harm standard").

To determine whether an impermissible use or disclosure of PHI constitutes a breach under this standard, CEs and BAs have been required to perform a risk assessment to determine if there is a significant risk of harm to the individual as a result of the impermissible use or disclosure. In conducting the risk assessment, CEs and BAs consider a number of factors, including who impermissibly used the information or to whom the information was impermissibly disclosed; whether the CE or BA had taken steps to mitigate or eliminate the risk of harm; whether the PHI was actually accessed; and what type or amount of PHI was impermissibly used or disclosed. The Interim Breach Notification Rule has required notification to be provided to each affected individual whose unsecured PHI was impermissibly used or disclosed (notification has also been required to be provided to the Secretary and, in certain cases, to the media).

As noted above, the Final Rule contains modifications to the provisions contained in the Interim Breach Notification Rule. First, the Final Rule contains a new definition of "breach." This new definition retains the exceptions from the definition

of breach contained in the Interim Breach Notification Rule,[12] but substantially revises the definition of breach. HHS notes that it revised this definition because it "recognize[s] the language used in the interim final rule and its preamble could be construed and implemented in manners [it] had not intended" and "some persons may have interpreted the risk of harm standard in the interim final rule as setting a much higher threshold for breach notification than we intended to set."

Under the Final Rule, "an impermissible use or disclosure of protected health information 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). Accordingly, HHS states that breach notification is necessary in all situations where there has been an impermissible use of disclosure of PHI, except for situations where the CE or BA, as applicable, demonstrates that there is a "low probability that the PHI has been compromised," or one of the exceptions to the definition of breach applies. HHS states that it believes that the express statement of this presumption in the Final Rule will help ensure that all CEs and BAs interpret and apply the Final Rule in a uniform manner.

In addition, the Final Rule incorporates what HHS refers to as a more "objective" risk assessment approach. Instead of assessing whether there is a significant risk of harm to the individual to determine whether breach notification is required, CEs and BAs must now assess the probability that PHI has been compromised. HHS notes that this risk assessment must consider at least the following factors, individually and in combination, as discussed below: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made; (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated. Thus, when performing a risk assessment under the Final Rule, a CE or BA, as applicable, must apply all of the four factors, as well as any other factors that may be necessary or appropriate in order to assess the risk that PHI was compromised.

HHS provides some guidance with respect to the four factors noted above. For example, with respect to the first factor, entities are advised to consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature, such credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. With respect to clinical information, HHS notes that sensitive information may include not only the nature of the services, but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results). Further, when assessing the second factor, HHS states that entities should consider whether the unauthorized person who received the

[12] The Interim Breach Notification Rule states: "(1) Breach excludes: (i) any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part; (ii) any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part; (iii) a disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information." 45 C.F.R. §164.402.

information has obligations to protect the privacy and security of the information. This factor should also be assessed in light of the risk of re-identification in the first factor to determine whether the unauthorized person may re-identify the information.

The third factor, according to HHS, requires CEs and BAs to investigate an impermissible use or disclosure to determine if the PHI was actually acquired or viewed or, alternatively, if only the opportunity existed for the information to be acquired or viewed (for example, if a forensic analysis of a recovered laptop that had been stolen shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised). Finally, HHS notes with respect to the fourth factor that CEs and BAs should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

As noted above, HHS states that a CE's or BA's analysis of the probability that PHI has been compromised following an impermissible use or disclosure must address each factor discussed above, as well as any other factors, as appropriate. CEs and BAs must then assess the overall probability that PHI has been compromised by considering all the factors in combination. HHS states that it expects the risk assessments "to be thorough, completed in good faith, and for the conclusions reached to be reasonable." If an evaluation of the factors fails to demonstrate that there is a low probability that the PHI has been compromised, breach notification is required. In addition, HHS notes that CEs and BAs may provide notification following an impermissible use of disclosure in violation of the Privacy Rule without performing a risk assessment.

In addition to the removal of the harm standard and the creation of more "objective" risk assessment factors, the Final Rule removes the exception for limited data sets that do not contain any dates of birth and zip codes. HHS indicates that this narrow exception had been included in the belief that it would be very difficult to re-identify a limited data set that excludes dates of birth and zip codes, and thus, a breach of such information would pose a low level of risk of harm to an individual. However, since this exception has been removed, following the impermissible use or disclosure of any limited data set, a CE or BA must perform a risk assessment that evaluates the factors discussed above to determine if breach notification is required.

Interestingly, HHS notes in the Final Rule that it will issue additional guidance in the future to aid CEs and BAs in performing risk assessments with respect to frequently occurring scenarios. In addition, HHS encourages CEs and BAs to "take advantage of the safe harbor provision of the breach notification rule" by encrypting limited data sets and other PHI pursuant to the Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.[13] If PHI is encrypted pursuant to this guidance, HHS notes, then no breach notification is required following an impermissible use or disclosure of the information.

[13] *See*, 74 Fed. Reg. 42740, 42742 (Aug. 24, 2009).

Notifications

In the Final Rule, HHS generally retains without modification provisions in the Interim Breach Notification Rule regarding the content of breach notifications, the method of such notifications, as well as the notification of individuals (§164.404). For example, HHS notes that it declined to adopt the suggestion that a CE be deemed to have discovered a breach only when management is notified of a breach. In addition, the Final Rule retains provisions regarding the notification of media (§164.406) without significant modification. With respect to notifying the Secretary of breaches (§164.408), the Final Rule makes a modification to the provisions contained in the Interim Breach Notification Rule in that it clarifies that CEs are required to notify the Secretary of all breaches of unsecured PHI affecting fewer than 500 individuals not later than 60 days after the end of the calendar year in which the breaches were "discovered," not in which the breaches "occurred."

With respect to notifications by a BA (§164.410), HHS notes that the Final Rule contains only "technical and nonsubstantive modifications" to the provisions contained in the Interim Breach Notification Rule. However, HHS provides important guidance regarding the timing of notifications depending on whether a BA is an agent of the CE. Specifically and as discussed in greater detail below, HHS notes that there are many different types of relationships that can develop between a CE and BA depending on the functions the BA performs on behalf of the CE. Accordingly, HHS states that if a BA is acting as an agent of the CE (based on the federal common law of agency), then the BA's knowledge of a breach is attributed to the CE and the CE is deemed to have knowledge of the breach as of the date the BA knew or, by exercising reasonable diligence, would have known of the breach. This means that the 60 days within which a CE must make notification begins to run when the *BA* knew or should have known of the breach, and not when the BA notifies the CE. The 60 days, then, generally will start to run well before the BA notifies the CE, often leaving the CE with much fewer than 60 days to make the required notifications.

However, if a BA is not an agent of the CE, then HHS notes that the 60-day period begins to run only when the CE is notified by the BA of the breach. In discussing this issue, HHS states that the use of the federal common law of agency to determine the BA's status with respect to the CE is consistent with the approach taken in the Final Rule's enforcement provisions for determining agency liability under the HIPAA Rules, discussed below. In addition, HHS encourages CEs and BAs to discuss and define in their BAAs the requirements regarding how, when, and to whom a BA should notify the CE of a potential breach.

III. The Enforcement Rule

In the Final Rule, HHS adopts many of the provisions contained in the Interim Enforcement Rule. It also, however, changes certain provisions that affect the imposition of Civil Monetary Penalties ("CMPs") and modifies certain provisions regarding HHS' conducting compliance audits and investigations. In the preamble to the Final Rule, HHS also provides important guidance regarding the liability of CEs for acts of their BA agents and determining agency liability.

JONES WALKER

e*bulletin

HEALTH CARE

February 2013 Vol. 17 healthcare@joneswalker.com

The Imposition of CMPs

As HHS notes, prior to the HITECH Act, the Secretary of HHS was authorized to impose a CMP of not more than $100 for a HIPAA violation, with the total amount imposed on a CE for all violations of an identical requirement or prohibition during a calendar year not to exceed $25,000. The HITECH Act changed this and established "tiers of increasing penalty amounts for violations based on increasing levels of culpability associated with each tier." This penalty scheme was then adopted in the Interim Enforcement Rule, and has now been adopted in the Final Rule.

As HHS also notes, the Interim Enforcement Rule established, and the Final Rule adopts, four tiers of increasing penalty amounts to correspond to the "levels of culpability" associated with a violation. The first category of violation (and lowest penalty tier) covers situations where the CE or BA did not know, and by exercising reasonable diligence would not have known, of a violation. The penalty associated with this tier is an amount not less than $100 or more than $50,000 for each violation. The second category of violation (and next highest penalty tier) applies to violations due to reasonable cause and not to willful neglect. The penalty associated with this tier is an amount not less than $1,000 or more than $50,000 for each violation. The third and fourth categories apply to circumstances where the violation was due to willful neglect that is timely corrected (second highest penalty tier) and willful neglect that is not timely corrected (highest penalty tier). The penalty associated with the third tier is an amount not less than $10,000 or more than $50,000 for each violation, while the penalty amount for the fourth tier is an amount not less than $50,000 for each violation. The penalty for violations of the same requirement or prohibition under any of these categories may not exceed $1,500,000 in a calendar year.

Factors in Determining the Amount of CMPs. In responding to commenters who were concerned about the Secretary's discretion regarding penalties that the Secretary could impose, HHS emphasizes that it will not impose the maximum penalty amount in all cases but will rather determine the amount of a penalty on a case-by-case basis, depending on factors including, without limitation, the nature and extent of the violation and the nature and extent of the resulting harm. More specifically, HHS lists the following five general factors the Secretary will consider in determining the amount of a CMP for a violation: (1) the nature and extent of the violation, including the number of individuals affected and the time period during which the violation occurred; (2) the nature and extent of the harm resulting from the violation, including financial, physical and reputational harm; (3) the history of prior compliance with the administrative simplification provision, including violations by the CE or BA; (4) the financial condition of the CE or BA; and (5) such other matters as justice may require.

In addition, HHS states that how violations are counted for purposes of calculating a civil money penalty will vary depending on the circumstances surrounding the noncompliance. Generally speaking, HHS notes that where multiple individuals are affected by an impermissible use or disclosure, it is "anticipated" that the number of identical violations of the Privacy Rule standard regarding permissible uses and disclosures would be counted by the number of individuals affected. In addition, with respect to continuing violations, HHS notes that it is anticipated that the number of identical violations of the safeguard standard would be counted on a per day basis (i.e., the number of days the entity did not have appropriate safeguards in place to protect the PHI).

Reasonable Cause. Although the Final Rule does not modify the tiers noted above and their associated penalty amounts, HHS commented that the "*mens rea*, or state of mind, associated with the tiers is clear with respect to the first, third, and fourth categories, in that there is no *mens rea* with respect to the lowest category of violation, while the existence of *mens rea* is presumed with respect to the third and fourth categories of violation." However, HHS notes that the state of mind requirement with respect to the second category of violation, or "reasonable cause," needed to be clarified. Accordingly, the Final Rule defines "reasonable cause" to mean "an act or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission violated an administrative simplification provision, but in which the covered entity or business associate did not act with willful neglect."

Thus, HHS explains that the definition of reasonable cause now includes violations due both to (1) circumstances that would make it unreasonable for the CE or BA, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated, as well as to (2) other circumstances in which a CE or BA has knowledge of a violation but lacks the conscious intent or reckless indifference associated with the willful neglect category of violations.

HHS Compliance Investigations and Reviews

The Final Rule makes a number of changes to certain provisions contained in the Interim Enforcement Rule with respect to HHS' investigation of complaints, HHS' conducting of compliance reviews, and the circumstances under which HHS will attempt to resolve investigations and compliance reviews by informal means.

First, HHS notes that the Interim Enforcement Rule has provided HHS with the discretion to investigate complaints made to the Secretary. More specifically, the Interim Enforcement Rule states that "the Secretary *may* investigate complaints" filed under §160.306. (Emphasis Added). The Final Rule, however, removes the discretion of the Secretary with respect to investigating complaints involving possible violations due to willful neglect. The Final Rule now provides that HHS *will* investigate all complaints when a preliminary review of the facts indicates a possible violation due to willful neglect. The Final Rule still provides the Secretary with the discretion to investigate any other complaints.

Similarly, HHS notes that the Interim Enforcement Rule has provided HHS with the discretion to conduct compliance reviews under §160.308 by stating that "the Secretary *may* conduct compliance reviews to determine whether covered entities are complying with the applicable administrative simplification provisions." (Emphasis Added). The Final Rule now removes this discretion and *requires* the Secretary to conduct a compliance review when a preliminary review of the facts indicates a possible violation due to willful neglect. The Final Rule, however, still provides the Secretary with the discretion to conduct a compliance review in any other circumstance.

Finally, HHS notes that the Secretary has been required under §160.312 to attempt to reach a resolution of an investigation of a complaint or a compliance review that indicates noncompliance by informal means. Under the Final Rule, HHS may, but is not required to, resolve such investigations and compliance reviews by informal means. HHS notes that this change permits HHS to proceed with a willful neglect violation determination as appropriate, while also permitting it to seek resolution of complaints and compliance reviews that did not indicate willful neglect violations by informal means. Further, HHS notes that, while that Secretary has been required to seek, to the extent practicable, the

cooperation of CEs in obtaining compliance with the HIPAA Rules, under the Final Rule, the Secretary would continue to do so "consistent with the provisions of this subpart" in recognition of the requirement to impose a CMP for a violation due to willful neglect. HHS states that "[w]hile the Secretary often will still seek to correct indications of noncompliance through voluntary corrective action, there may be circumstances (such as circumstances indicating willful neglect), where the Secretary may proceed directly to formal enforcement."

The Agency Relationship

Importantly, the Final Rule removes an exception in the Interim Enforcement Rule that limited the liability of CEs for CMPs for the acts of its agents in certain circumstances. Specifically, §160.402(c) has provided that, although a CE is liable, in accordance with the federal common law of agency, for a civil money penalty for a violation based on the act or omission of any agent of the CE acting within the scope of the agency, the CE was *not* liable for the acts of its agent in cases where (1) the agent was a BA; (2) the relevant contract requirements were met; (3) the CE did not know of a pattern or practice of the BA in violation of the contract; and (4) the CE did not fail to act as required by the Privacy or Security Rule with respect to such violations.

HHS notes that the Final Rule now provides that CEs and BAs are liable for the acts of their agents, in accordance with the federal common law of agency, regardless of whether there is a compliant BAA or contract in place. According to HHS, one reason for the removal of the exception is to ensure that where a CE or BA has delegated out an obligation under the HIPAA Rules, the CE or BA would remain liable for penalties for the failure of its BA agent to perform the obligation on the CE or BA's behalf.

In the Final Rule, HHS specifically declines to provide definitions of "principal," "agent," and "scope of agency." Instead, it directs entities to refer to the federal common law of agency to determine the definitions and application of the terms. Thus, HHS notes that an analysis of whether a BA, or a BA subcontractor, is an agent will be fact specific, and will take into account the terms of a BAA or contract "as well as the totality of the circumstances involved in the ongoing relationship between the parties." According to HHS, the essential factor in determining whether an agency relationship exists between a CE and its BA (or BA subcontractor) is the right or authority of a CE to control the BA's (or BA subcontractor's) conduct in the course of performing a service on behalf of the CE.

In an attempt to shed light on the issue of agency, HHS provides guidance as to when an agency relationship would likely be created. For example, HHS states that the authority of a CE to give interim instructions or directions is the type of control that distinguishes CEs in agency relationships from those in non-agency relationships. If, according to HHS, the only avenue of control is for a CE to amend the terms of the BAA or contract, or to sue for breach of contract, this generally indicates that a BA is *not* acting as an agent. In contrast, a BA generally *would* be an agent if it the BAA granted the CE the authority to direct the performance of the service provided by its BA after the relationship was established. For example, HHS notes that if the terms of a BAA state that "a business associate must make available protected health information in accordance with §164.524 based on the instructions to be provided by or under the direction of a covered entity," then this would create an agency relationship between the CE and BA for this activity because the CE has a right to give interim instructions and direction during the course of the relationship.

Further, HHS lists several factors that are important to consider in any analysis to determine the scope of agency, including: (1) the time, place, and purpose of a BA agent's conduct; (2) whether a BA agent engaged in a course of conduct subject to a CE's control; (3) whether a BA agent's conduct is commonly done by a BA to accomplish the service performed on behalf of a CE; and (4) whether or not the CE reasonably expected that a BA agent would engage in the conduct in question. Other factors that HHS notes are important to the determination include, without limitation, the type of service and skill level required to perform the service, and whether the CE is legally or otherwise prevented from performing the service or activity performed by its BA.

HHS also notes that an agency relationship can be established despite the terms and labels the parties use in a contract (e.g., independent contractor). Agency can also be established despite the fact that the CE does not retain the right or authority to control every aspect of its BA's activities, and regardless of whether the CE actually exercises the right of control. It is enough if the CE has the authority to exercise such right. Finally, HHS states that even if a CE and its BA are separated by physical distance, an agency relationship may be established (e.g., if a CE and BA are located in different countries).

IV. Next Steps

It is clear from the number of changes set forth above that CEs and BAs have much to consider and to accomplish in the coming months. Relationships between CEs and BAs, as well as relationships between BAs and BA subcontractors need to be examined. BAAs will need to be carefully reviewed and revised as necessary to comply with the Final Rule. The extension of BAs to include downstream entities will necessitate that BAs enter into agreements with these entities, and CEs will need to ensure that their BAAs cover such relationships. Policies and procedures will need to be reviewed and substantially revised to include, without limitation, the new definition of breach and the breach assessment standards. Of course, the foregoing changes will also require entities to quickly train all workforce personnel, as well as potentially other individuals such as members of a CE's medical staff, with respect to the new requirements contained in the Final Rule.

Jones Walker is available to assist with any and all of the steps that need to be taken as a result of the myriad changes set forth in the Final Rule. In addition, as noted above, Part II of our analysis of certain changes to the HIPAA Rules will include discussions of marketing, fundraising, the sale of PHI, authorizations, research, access to PHI, modifications as result of GINA, and the Notice of Privacy Practices.

Please join us for our Health Care Seminar, which will be held in Hollywood, Florida, on Friday, March 15, 2013, where we will discuss, among other topics such as quality of care in physician arrangements and how to survive a ZPIC review, the "down and dirty" on the new HIPAA Final Rule. For more information, please contact Lynn M. Barrett at lbarrett@joneswalker.com.

— Lynn M. Barrett, Esq.

JONES WALKER

e*bulletin

HEALTH CARE

February 2013 Vol. 17 healthcare@joneswalker.com

Jones Walker offers a broad range of legal services to health care industry clients, including regulatory compliance, litigation, investigations, operations, and transactional matters. These legal principles may change and vary widely in their application to specific factual circumstances. You should consult with counsel about your individual circumstances. For further information regarding these issues, contact:

Myla R. Reizen
Jones, Walker, Waechter, Poitevent, Carrère & Denègre L.L.P.
Miami Center, Suite 2600
201 S Biscayne Boulevard
Miami, FL 33131-4341
305.679.5716 *tel*
305.679.5710 *fax*
mreizen@joneswalker.com

Health Care Attorneys

Lynn M. Barrett
Allison C. Bell
George F. Bloss, III
David P. Borghardt
Amy C. Cowley
Mark A. Cunningham
Nadia de la Houssaye
Kathryn W. Drey
Stephanie C. Edgar
S. Trent Favre
Pauline F. Hardin
Kathleen A. Harrison
Kathryn H. Hester
Robert B. House
Mary Margaret Kuhlmann
Joseph J. Lowenthal, Jr.
J. Leray McNamara
James C. Percy
David G. Radlauer
Rudolph R. Ramelli
Myla R. Reizen
Krystal Pfluger Scott
Donald W. Washington
Amy M. Winters

To subscribe to other E*Bulletins, visit http://www.joneswalker.com/ecommunications.html.