

# HEALTH LAW UPDATE

NEWS FOR THE CLIENTS AND FRIENDS OF BASS, BERRY & SIMS PLC

## **Tough New Era for Business Associates and Their Subcontractors: HHS Issues Proposed Modifications to HIPAA Privacy, Security and Enforcement Rules**

**July 13, 2010**

On July 8, 2010, the Department of Health and Human Services (HHS) issued a Notice of Proposed Rulemaking (NPRM) to modify the HIPAA<sup>1</sup> Privacy, Security and Enforcement Rules (the HIPAA Rules). The NPRM addresses certain modifications to the HIPAA Rules required by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, and proposes additional changes to HIPAA that are not statutorily mandated by the HITECH Act but that, in HHS' view, would make the HIPAA Rules more effective and workable. If finalized, these changes will require revisions to business associate agreements (BAAs) and Notices of Privacy Practices (NPPs) for protected health information (PHI) and will subject business associates and their subcontractors to direct liability under the HIPAA Rules.

The NPRM will be published in the *Federal Register* on July 14, 2010, and HHS will accept public comments on the proposed rule for 60 days thereafter.

### **Proposed 180-day Compliance Period for Privacy and Security Rule Modifications**

Although most provisions of the HITECH Act became effective February 18, 2010, the final rule implementing the modifications to the HIPAA Rules will take effect 180 days from the effective date of the final rule addressing these issues. HHS has proposed this extended compliance period to allow covered entities and business associates time to implement the changes necessary to come into compliance with their obligations under the final rule (with the exception of the required changes to BAAs, as discussed below).

### **Modified Business Associate Agreement Requirements; Amendments Likely Required**

The NPRM proposes several modifications to the requirements for a compliant BAA. For example, the NPRM would require BAAs to obligate business associates to report breaches of unsecured PHI. Many covered entities and business associates have entered into BAAs since the enactment of the HITECH Act that address the obligation to report such breaches. However, the NPRM proposes to add an element to the list of required BAA provisions that existing agreements are unlikely to address. Specifically, the rule would require BAAs to state that to the extent that the business associate carries out the covered entity's obligations with respect to the privacy of PHI, the business

---

<sup>1</sup> The Health Insurance Portability and Accountability Act of 1996.

associate will comply with the requirements of the privacy rule that apply to the covered entity. In other words, although the HITECH Act made business associates directly liable for certain provisions of the Privacy Rule, this added provision would require BAAs to also make business associates contractually liable for obligations of the covered entity handled by the BAA. Given the direct liability of business associates under the Privacy Rule as a result of the HITECH Act, it is difficult to justify the administrative burden on covered entities and business associates that this proposal will create.

At this time, covered entities and business associates are advised to wait for publication of the final rule before amending existing BAAs, assuming their BAAs already comply with the existing HIPAA Rules. However, covered entities and business associates may wish to revise their BAA templates now to reflect the proposed modifications to reduce the administrative and financial burden in the event that the proposed rules are finalized.

### **One-Year Transition Period for BAAs**

As discussed above, the proposed additions and amendments to BAAs, if made final, will likely require covered entities and business associates to revise their BAA forms going forward as well as to amend and potentially renegotiate their existing BAAs. Recognizing the anticipated cost and burden of implementing the revised BAA rules, HHS proposes to allow for a transition period for certain existing BAAs. If this proposal is finalized, covered entities and business associates that already have in place BAAs that comply with the existing HIPAA Rules will have one year from the compliance date of the final rule to amend their existing BAAs, except that if the parties amend or renew their existing contracts during the one-year transition period, they will need to revise their BAAs at that time. If a contract renews automatically, the period of deemed compliance would not end when the contract automatically rolls over but will continue until expiration of the one-year transition period.

Those covered entities and business associates currently using BAAs that do not comply with the existing HIPAA Rules would not be able to take advantage of the one-year transition period. Any covered entity or business associate that does not have compliant BAAs in place should act quickly to remedy the deficiency, both to avoid liability under the existing HIPAA Rules and to be able to take advantage of the one-year transition period should the NPRM be finalized.

### **Expanded Application of the HIPAA Rules to Downstream Subcontractors**

The NPRM proposes to revise the definition of business associate to include a subcontractor that receives or handles PHI on behalf of a business associate. If this proposal is finalized, downstream entities that work on behalf of a business associate and that create or receive PHI on behalf of the business associate would be required to comply with, and subject to liability under, the HIPAA Rules in the same manner as the business associate. Thus, downstream entities would also be directly liable for acts of noncompliance. Further, liability would extend to subcontractors of downstream entities (and subcontractors of those subcontractors) to the extent these entities created or received PHI.

The NPRM would not require covered entities to have in place contracts with these downstream entities. Business associates, however, would be obligated to implement BAAs with each of their subcontractors that handle PHI to ensure that the subcontractor will comply with the HIPAA Rules. To use an example offered by HHS, if a business associate employs the services of a company for document shredding and secure disposal of PHI, the shredding company would be directly obligated to implement safeguards with respect to handling the PHI, as well as to limit its uses and disclosures

of the PHI, and the business associate would be required to ensure that the company agrees in writing to adhere to the applicable privacy and security provisions of the HIPAA Rules.

The NPRM would require BAAs between business associates and subcontractors to contain the same provisions as BAAs between covered entities and business associates. Although business associates are already contractually required to enter into these downstream BAAs with subcontractors, the NPRM would make this a regulatory requirement. The revised provisions for BAAs between business associates and covered entities, discussed above, would also apply to agreements between business associates and subcontractors. Therefore, business associates should be prepared to revise existing downstream BAA templates and to amend existing BAAs with their subcontractors as needed. The proposed one-year transition period discussed above would also apply to business associates and their subcontractors.

### **Revised Notices of Privacy Practices for Protected Health Information**

The HIPAA Rules require most covered entities to provide individuals with an NPP, which must describe the uses and disclosures of PHI a covered entity is permitted to make, the covered entity's legal duties and privacy practices with respect to PHI, and the individuals' rights concerning their PHI. The NPRM proposes certain changes and additions to the content of a covered entity's NPP. First, the rule would require that the NPP include a statement describing certain examples of uses and disclosures of PHI that require an authorization (specifically, uses and disclosures for psychotherapy notes, for marketing, and for the sale of PHI). Currently, NPPs are required to state that uses or disclosures not described in the NPP will be made only with the individual's authorization, but are not required to describe examples of uses or disclosures requiring an authorization. The NPRM would also require the NPP to include certain specific statements regarding the covered entity's communications related to marketing, fundraising and subsidized treatment, all of which are intended to conform to HHS' proposed modifications to the HIPAA Rules. Further, NPPs will be required to include a statement that a covered entity is not required to agree to a restriction request, except for requests by self-pay patients to restrict disclosures to health plans for purposes of treatment, payment or healthcare operations.

These proposed amendments to NPPs, if finalized, represent material changes. Therefore, covered entities would be required to revise and redistribute their NPPs to individuals. In the case of a health plan, the covered entity is required to provide notice to individuals covered by the plan within 60 days of a material change to an NPP. Recognizing the cost and burden associated with this obligation, HHS requests comments on certain options for implementing these changes, such as extending the timeframe for compliance for health plans. Covered entities should be prepared to revise their NPPs to come into compliance with the HIPAA modifications, but are advised to wait until the publication of the final rule to make specific changes to their content.

### **Other Provisions of the NPRM**

In addition to the changes discussed above, business associates and covered entities should be aware of certain additional HIPAA Rule modifications proposed by HHS, which include the following:

- Adding two exceptions to the prohibition on the sale of PHI without an authorization from the individual: (1) for disclosures required by law, and (2) for disclosures made for any other purpose as long as the only remuneration received by the covered entity is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee is permitted by law.

- Strengthening the ability of an individual to "opt out" of receiving any fundraising and marketing communications from a covered entity by requiring that the covered entity provide a simple, quick and inexpensive method for individuals to opt out, such as through the use of a toll-free number or e-mail address (in contrast, requiring individuals to mail letters requesting to opt out would not be deemed quick and inexpensive).
- Modifying the definition of *marketing* to provide that healthcare operations communications for which the covered entity receives financial remuneration would be considered *marketing* and would require individual authorization to make the communication. HHS is also seeking comments on the scope of the exceptions to marketing activities that may be considered permissible *treatment* or *healthcare operations* communications.
- Requesting comment on the implementation of provisions regarding the rights of individuals to access their information and to restrict certain types of disclosures of PHI to health plans, both of which rights were strengthened under the HITECH Act.
- Requesting comment on whether, with the advance of electronic health records, the timeliness standard for responding to an individual's access request should be altered generally or with respect to records stored electronically. Currently, a covered entity has up to 30 days to respond, with the ability to extend the response time by 30 days. In the context of defining "meaningful use" of electronic health records technology, HHS has proposed requiring that individuals be provided electronic access to their health information (including lab results and medication lists) within 96 hours of the information's being available to the treating physician.<sup>2</sup>
- Modifying the definition of PHI to provide that the HIPAA Rules would not apply to individually identifiable health information of persons who have been deceased for more than 50 years. This provision would benefit researchers and others seeking to access archived PHI without the burden of attempting to obtain authorizations from personal representatives of those who have long been deceased.
- Amending the definition of certain terms related to enforcement of the HIPAA Rules. For example, HHS proposes to amend the definition of reasonable cause to recognize those circumstances that make it unreasonable for a covered entity or business associate to comply with the provision that was violated, despite the exercise of ordinary business care and prudence. The NPRM also proposes clarifications to and provides examples for certain categories of *mens rea* for HIPAA violations, such as *knowledge* and *willful neglect*.
- Adding a provision that a business associate is liable for a HIPAA violation based on the act or omission of any agent of the business associate, including workforce members or subcontractors acting within the scope of their agency relationships.
- Making explicit the statutory requirement under the HIPAA Enforcement Rule that the Secretary of HHS may consider the nature and extent of the HIPAA violation and the nature of the harm resulting from the HIPAA violation in determining the appropriate penalty amount.
- Revising language of the HIPAA Rules, where applicable, to reflect the HITECH Act's extension of certain provisions of these Rules to business associates.

---

<sup>2</sup> See 75 Fed. Reg. 1844, 1857 (January 13, 2010).

The NPRM does not propose to modify the interim final rule issued on August 24, 2009, regarding Breach Notification for Unsecured Protected Health Information.

If you have questions about any aspect of the NPRM, the HITECH Act, or the HIPAA Rules in general, or would like assistance with drafting comments to the NPRM, please contact any of the attorneys in our Healthcare Practice Group listed below.

**Bass, Berry & Sims Healthcare Attorneys**

**H. Lee Barfield, II**  
(615) 742-6202  
[lbarfield@bassberry.com](mailto:lbarfield@bassberry.com)

**Philip F. Berg**  
(615) 742-7908  
[pberg@bassberry.com](mailto:pberg@bassberry.com)

**Krista Thornton Cooper**  
(615) 742-7734  
[kcooper@bassberry.com](mailto:kcooper@bassberry.com)

**Meredith Edwards**  
(615) 742-7823  
[medwards@bassberry.com](mailto:medwards@bassberry.com)

**Mary Beth Fortugno**  
(615) 742-7739  
[mfortugno@bassberry.com](mailto:mfortugno@bassberry.com)

**Valere Fulwider**  
(615) 742-7822  
[vfulwider@bassberry.com](mailto:vfulwider@bassberry.com)

**Lauren Gaffney**  
(615) 742-7824  
[lgaffney@bassberry.com](mailto:lgaffney@bassberry.com)

**Pooneh Ghiassi**  
(615) 742-7782  
[pghiassi@bassberry.com](mailto:pghiassi@bassberry.com)

**Anna Grizzle**  
(615) 742-7732  
[agrizzle@bassberry.com](mailto:agrizzle@bassberry.com)

**Elisa E. Harris**  
(615) 742-6553  
[eharris@bassberry.com](mailto:eharris@bassberry.com)

**Angela Humphreys**  
(615) 742-7852  
[ahumphreys@bassberry.com](mailto:ahumphreys@bassberry.com)

**J. James Jenkins, Jr.**  
(615) 742-6236  
[jjenkins@bassberry.com](mailto:jjenkins@bassberry.com)

**Seth A. Killingbeck**  
(615) 742-7707  
[skillingbeck@bassberry.com](mailto:skillingbeck@bassberry.com)

**David King**  
(615) 742-7890  
[dking@bassberry.com](mailto:dking@bassberry.com)

**Claire F. Miley**  
(615) 742-7847  
[cmiley@bassberry.com](mailto:cmiley@bassberry.com)

**T. Scott Noonan, Co-Chair**  
(615) 742-6273  
[snoonan@bassberry.com](mailto:snoonan@bassberry.com)

**Shannon Pinkston**  
(615) 742-7727  
[spinkston@bassberry.com](mailto:spinkston@bassberry.com)

**Cynthia Y. Reisz**  
(615) 742-6283  
[creisz@bassberry.com](mailto:creisz@bassberry.com)

**Brian D. Roark**  
(615) 742-7753  
[broark@bassberry.com](mailto:broark@bassberry.com)

**Catherine J.B. Sloan**  
(615) 742-7789  
[csloan@bassberry.com](mailto:csloan@bassberry.com)

**Danielle M. Sloane**  
(615) 742-7763  
[dsloane@bassberry.com](mailto:dsloane@bassberry.com)

**Nesrin Garan Tift**  
(615) 742-7903  
[ntift@bassberry.com](mailto:ntift@bassberry.com)

**Leigh Walton, Co-Chair**  
(615) 742-6201  
[lwalton@bassberry.com](mailto:lwalton@bassberry.com)

**Elizabeth S. Warren**  
(615) 742-7719  
[ewarren@bassberry.com](mailto:ewarren@bassberry.com)

**Douglas M. Wolford**  
(615) 742-7917  
[dwolford@bassberry.com](mailto:dwolford@bassberry.com)

*The materials contained herein have been abridged from the statutory sources and should not be construed or relied upon for legal advice. Readers are urged to consult legal counsel concerning particular situations and specific legal questions.*

*To ensure compliance with requirements imposed by the IRS, we inform you that this message is not intended to be used, and cannot be used, by the addressee or any other person for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code.*

150 Third Avenue South, Suite 2800 • Nashville, TN 37201 • (615) 742-6200

The Tower at Peabody Place • 100 Peabody Place, Suite 900 • Memphis, TN 38103 • (901) 543-5900

1700 Riverview Tower • 900 South Gay Street • Knoxville, TN 37902 • (865) 521-6200