

HEALTH LAW

Update

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

Breach of Unsecured Personal Health Information: New Notice Requirements

August 28, 2009

On August 24, 2009, the Department of Health and Human Services ("HHS") published an interim final rule implementing new notification requirements for breaches of unsecured protected health information ("PHI").¹ The rule requires covered entities² to report breaches to affected individuals without unreasonable delay but no later than 60 days of discovery of the breach (and requires business associates³ to report breaches to their covered entities without unreasonable delay but in no case later than 60 days after discovery of the breach). Covered entities must also notify HHS within 60 days of discovery for large breaches, i.e., those affecting 500 or more individuals, and must notify HHS annually for those impacting fewer than 500 individuals. In some cases, notification to the media is required, as well.

Importantly, covered entities and their business associates only have 30 days (until September 23, 2009) to come into compliance with the rule. Although HHS has created a 180 day enforcement discretion period, during which it will not impose sanctions for failures to provide notices for breaches discovered during the 180 day period, HHS clearly states in the preamble to the rule that it expects covered entities and business associates to comply with the rule beginning September 23, 2009.⁴ Thus, swift action is required in order to implement the rule's requirements.

As discussed in more detail below, covered entities and their business associates need to:

- (1) prepare policies and procedures that track the rule's requirements, including mechanisms to identify and report potential breaches internally; promptly investigate reports of potential breaches; in the event of a breach, send required notices to individuals and HHS and, in some cases, the media; and document breaches and any determinations that an incident does not require notification;

¹ 74 Fed. Reg. 42740 (creating 45 CFR Part 164, Subpart D).

² A *covered entity* under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a health plan, health care clearinghouse or health care provider that transmits health information electronically in connection with a transaction covered by HIPAA. *See* 45 CFR § 160.103.

³ A *business associate* under HIPAA is person or entity that performs functions or activities on behalf of a covered entity that involves the use or disclosure of PHI. *See* 45 CFR §160.103.

⁴ 74 Fed. Reg. at 42756-57.

- (2) update existing policies issued under the HIPAA Privacy Rule⁵ to address the breach reporting rule;
- (3) determine whether to amend existing business associate agreements to address the breach reporting rule expressly; and
- (4) train all affected workforce members on the need to report immediately any potential breaches.

Background on the Rule/Additional Changes Possible

Enacted on February 17, 2009, the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act")⁶ strengthened the privacy and security requirements of HIPAA by increasing penalties for violations and placing added obligations on covered entities and business associates. The HITECH Act also created a federal reporting requirement for breaches involving unsecured PHI. Previously, breach reporting requirements have been state-by-state and have been generally aimed at preventing identity theft, rather than focused on PHI.

The breach reporting rule was issued as an interim final rule, meaning HHS did not issue a proposed rule on which covered entities, business associates or others could submit comments. However, HHS will accept comments on the interim final rule until October 23, 2009. Thus, it is possible that HHS will revise the breach reporting rule in response to any comments it receives.

Reportable Breaches

The reporting obligation is triggered when there is a breach of unsecured PHI. To that end, the definitions of *breach* and *unsecured PHI* are critical.

For purposes of the breach reporting rule, *breach* is broadly defined as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [the HIPAA Privacy Rule] which compromises its security or privacy."⁷ Thus, any use or disclosure of PHI not permitted by the HIPAA Privacy Rule, such as a request for PHI that is more than minimally necessary for the purpose of the request, could trigger a breach reporting obligation. However, HHS created five exceptions or carve-outs from the definition of *breach* that will narrow the notification obligation and avoid having to notify individuals of minor failures to comply with the HIPAA Privacy Rule:

- (1) *Incidents that do not pose a significant risk of harm.* To be reportable, an incident must pose a significant risk of financial, reputational, or other harm to the individual.⁸ In order to determine whether this "harm" threshold has been reached as a result of an impermissible use or disclosure of PHI, covered entities and business associates will need to perform, and document the outcome of, a risk assessment. The risk assessment should include such factors as *who* used or received the information, *what type* of information was involved (*i.e.*, is it highly sensitive PHI?), whether immediate and effective steps to mitigate the incident were taken (such as receiving

⁵ 45 CFR Part 160 and Part 164, Subparts A and E.

⁶ The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009.

⁷ 45 CFR § 164.402.

⁸ 45 CFR § 164.402.

assurances from the recipient that the PHI was destroyed) and whether the PHI was returned prior to being accessed for an improper purpose.⁹ For example, HHS recognizes that there is less risk of harm when PHI is improperly disclosed to another covered entity, since the recipient has an independent duty to protect the information.

- (2) Practically de-identified information. Disclosures of PHI that do not include an individual's date of birth or zip code and that meet the requirements to be considered a limited data set¹⁰ are deemed not to compromise the security or privacy of PHI and are not reportable.¹¹
- (3) Certain unintentional uses. Notification is not required for any unintentional use, access, or acquisition of PHI by a workforce member or individual acting under the authority of a covered entity or business associate, if the acquisition, access or use was made in good faith, within the scope of authority and does not result in further use or disclosure not permitted under the HIPAA Privacy Rule.¹² For example, notification is not required when a billing employee at a hospital mistakenly receives an email containing PHI, immediately deletes the email and alerts the sender of the mistake.
- (4) Certain inadvertent disclosures. Notification is not required for any inadvertent disclosure of PHI by a person who is authorized to access PHI at the covered entity or business associate if the recipient is authorized to access PHI at the same covered entity or business associate or organized health care arrangement, and the disclosed PHI is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.¹³
- (5) Incidents involving no ability to retain the PHI. Notification is not required when the covered entity or business associate has a good faith belief that the recipient was not reasonably able to retain the PHI.¹⁴ According to HHS, an example of this situation would be a covered entity that mails a number of explanation of benefits ("EOBs") to the wrong individuals, but the EOBs are returned unopened by the post office as undeliverable.

The term *unsecured* PHI is defined to mean PHI "that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by" HHS pursuant to the HITECH Act and as set forth on its website.¹⁵ On April 17, 2009, HHS issued guidance identifying two methods for "securing" PHI: encryption and destruction. In the preamble to the rule, HHS updates this earlier guidance by specifying that electronic PHI has been sufficiently secured if it has been encrypted by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential

⁹ 74 Fed. Reg. at 42744-45.

¹⁰ The limited data set requirements are found at 45 CFR § 164.514(e)(2). A limited data set is information that is almost de-identified information.

¹¹ 45 CFR § 164.402.

¹² 45 CFR § 164.402. The regulations replace the word "employee" as used in the HITECH Act with the phrase "workforce member," to encompass volunteers and trainees as well as employees.

¹³ 45 CFR § 164.402.

¹⁴ 45 CFR § 164.402.

¹⁵ 45 CFR § 164.402; the guidance can be found at <http://www.hhs.gov/ocr/privacy/>.

process or key," and if such decryption tools are stored securely.¹⁶ Destruction will be sufficient for electronic media if they have been cleared or purged. Paper or film media will be sufficiently destroyed if they have been shredded or destroyed such that PHI cannot be reconstructed. HHS specifies that redaction of paper, film, or hard copy media will not be sufficient.¹⁷

Notification Obligations for Covered Entities

If a covered entity discovers a breach of unsecured PHI, it must notify each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed as the result of the breach.¹⁸ Notification is due without unreasonable delay but in no case more than 60 days following discovery of the breach.¹⁹ A breach is treated as "discovered" by a covered entity on the first day the breach is known, or would have been known with reasonable diligence, by any person (other than the person committing the breach) who is a workforce member *or agent* of the covered entity.²⁰ This aggressive interpretation creates a significant risk that a covered entity will inadvertently miss the 60 day deadline due to a workforce member or agent who delays in reporting a potential breach to his or her supervisor or the entity's privacy officer. Covered entities should ensure that their workforce members and agents are well-trained on how to identify and immediately and appropriately report potential breaches.

HHS acknowledges that not all business associates will be considered agents. For business associates who are not agents (based on federal common law of agency), the 60 day period will begin when the covered entity is notified by the business associate of the breach.²¹

A covered entity must delay notification of a breach if a law enforcement official states that notification would impede a criminal investigation or cause damage to national security.²² The 60-day period is tolled until the time period specified in the law enforcement official's written statement to the covered entity or, in the case of oral statements, for 30 days unless a written statement is submitted by the law enforcement official during that 30 day period.

Content and Method of Notification

The notification to individuals must be written in plain language and contain the following items, to the extent possible: (1) a brief description of what happened, including date of the breach and date of discovery of the breach, if known; (2) a description of the types of unsecured PHI that were involved (such as name, social security number and date of birth); (3) the steps individuals should take to protect themselves from potential harm resulting from the breach; (4) a brief description of what the covered entity is doing to investigate the breach, mitigate harm to the individual and protect against any further breaches; and (5) contact procedures for individuals to ask questions or learn additional

¹⁶ 74 Fed. Reg. at 42742-43.

¹⁷ 74 Fed. Reg. at 42743. However, HHS acknowledged that incidents involving redacted information might not trigger a notification obligation if the covered entity determines the redacted information meets the requirements to be considered de-identified or if the incident does not compromise the security or privacy of PHI. 74 Fed. Reg. at 42742.

¹⁸ 74 Fed. Reg. at 42768.

¹⁹ 74 Fed. Reg. at 42768.

²⁰ 45 CFR § 164.404(a).

²¹ 74 Fed. Reg. at 42754.

²² 45 CFR § 164.412.

information, which must include a toll-free telephone number, email address, website, or postal address.²³

The method of notification varies based on the scope of the breach and whether the covered entity has up-to-date contact information. Regardless of the number of affected individuals, the covered entity must notify individuals in writing by first-class mail delivered to the last known address of the individual or in the form of e-mail if the individual has agreed to receive notice in electronic format.²⁴ If the breach involves information of 10 or more individuals for whom the covered entity has insufficient or out-of-date contact information, the covered entity must providing "substitute notice" by disclosing the breach on the homepage of its website for 90 days or by placing a conspicuous notice in major print or broadcast media where the individuals are likely to reside. In either case, the substitute notice must include a toll-free number where individuals can learn whether their information was accessed by the breach. If the breach involves fewer than 10 individuals for whom the covered entity lacks up-to-date contact information, the substitute notice may be provided by written notice, telephone or "other means." In any case that a covered entity deems to require urgency due to possible imminent misuse, a covered entity may contact individuals by telephone or other means in addition to providing the required notice described above.²⁵

In the case of a breach involving any 500 or more individuals, the covered entity must notify the Secretary of HHS at the same time that individuals are notified. For breaches involving 500 or fewer individuals, covered entities must document the breaches and report a log of the breaches for the previous calendar year to the Secretary within 60 days of the end of the calendar year.²⁶ For calendar year 2009, covered entity must submit a log of breaches involving less than 500 people occurring on or after September 23, 2009 (even though HHS has agreed to delay imposing penalties for failure to comply for 180 days (until February 22, 2010)).²⁷

If the breach involves information of more than 500 residents of any state or jurisdiction, the covered entity must notify prominent media outlets of that state or jurisdiction.²⁸ This notice must be made within 60 days of the date of discovery of the breach. The term *prominent media outlets* is not defined.

Notification Obligations of Business Associates

If a business associate discovers a breach of unsecured PHI, it must notify the covered entity of the breach without unreasonable delay, but in no case later than 60 days following the discovery of the breach. The same interpretation for "discovery" discussed above for covered entities will apply to business associates.²⁹ To the extent possible, the business associate's notice to the covered entity must identify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired, used or disclosed and any other information known to the business associate that the covered entity will be required to include in the notification to affected individuals.³⁰ HHS acknowledges that in some situations, business associates may be unable to identify individuals

²³ 45 CFR § 164.404(c).

²⁴ 45 CFR § 164.404(d).

²⁵ 45 CFR § 164.404(d)(3).

²⁶ 45 CFR § 164.408.

²⁷ 74 Fed. Reg. at 42753.

²⁸ 45 CFR § 164.406.

²⁹ See 45 CFR § 164.410(a)(2).

³⁰ 45 CFR § 164.410(c).

affected by a breach, such as a records storage company that holds boxes containing voluminous paper medical records on behalf of a covered entity. In this type of situation, if several boxes go missing, HHS recognizes that the covered entity would be better positioned to identify the individuals affected by the breach.³¹

Business associates are required to delay notification to the covered entity if instructed to do so by a law enforcement official, as discussed above with respect to covered entities.

State Laws Remain in Place

A majority of states have enacted security breach notification laws that apply not only to covered entities and business associates but also to any entity that maintains personal information. The federal breach reporting rule will preempt any contrary provision of state law unless the state law is more stringent with respect to protecting the privacy of PHI. A state law is deemed to be contrary to the federal rule if a covered entity would find it impossible to comply with both the state and federal requirements or if the state law stands as an obstacle to accomplishing the objectives of the federal breach reporting rule.³² HHS takes the position that covered entities should generally be able to comply with both state laws and the federal breach reporting rule.³³ Therefore, covered entities faced with a breach will have to comply with the federal breach reporting rule and determine whether they are subject to additional or more stringent breach reporting standards under state law, which is especially challenging for breaches that impact residents of more than one state.

HIPAA Privacy Rule Changes

HHS made conforming changes to the HIPAA Privacy Rule administrative requirements to include references to the new breach reporting requirement. Thus, covered entities must implement policies, train workforce members on their policies, impose sanctions on workforce members who violate these policies, permit individuals to file complaints regarding compliance with the breach reporting rule, not require individuals to waive their rights under the breach reporting rule and refrain from retaliatory acts.³⁴ Covered entities should already have policies in place that address each of these requirements with respect to the HIPAA Privacy Rule, but should review and revise their policies to reference clearly the breach reporting rule. Covered entities should also review their business associate agreement templates to determine whether existing requirements to report non-permissible uses and disclosures are sufficiently detailed.

If you have any questions regarding this Health Law Update or would like assistance with your compliance efforts or in preparing comments to the rule to submit to HHS, please contact any attorney in our Healthcare Practice Group listed below.

³¹ 74 Fed. Reg. at 42754.

³² See 45 CFR § 160.202.

³³ 74 Fed. Reg. at 42756.

³⁴ 45 CFR § 164.530.

Bass, Berry & Sims Healthcare Attorneys

H. Stanford Adams, Jr.
(615) 742-7775
sadams@bassberry.com

H. Lee Barfield, II
(615) 742-6202
lbarfield@bassberry.com

Philip F. Berg
(615) 742-7908
pberg@bassberry.com

Krista Thornton Cooper
(615) 742-7734
kthornton@bassberry.com

Mary Beth Fortugno
(615) 742-7739
mfortugno@bassberry.com

Pooneh Ghiassi
(615) 742-7782
pghiassi@bassberry.com

Anna Grizzle
(615) 742-7732
agrizzle@bassberry.com

Elisa E. Harris
(615) 742-6553
eharris@bassberry.com

Angela Humphreys
(615) 742-7852
ahumphreys@bassberry.com

Clevonne M. Jacobs
(615) 742-7769
vjacobs@bassberry.com

J. James Jenkins, Jr.
(615) 742-6236
jjenkins@bassberry.com

Seth A. Killingbeck
(615) 742-7707
skillingbeck@bassberry.com

David King
(615) 742-7890
dking@bassberry.com

Claire F. Miley
(615) 742-7847
cmiley@bassberry.com

T. Scott Noonan, Co-Chair
(615) 742-6273
snoonan@bassberry.com

Brenda N. Phillips
(615) 742-6237
bnphillips@bassberry.com

Shannon Pinkston
(615) 742-7727
spinkston@bassberry.com

Cynthia Y. Reisz
(615) 742-6283
creisz@bassberry.com

Brian D. Roark
(615) 742-7753
broark@bassberry.com

Scott B. Shanker
(901) 543-5932
sshanker@bassberry.com

Catherine J.B. Sloan
(615) 742-7789
csloan@bassberry.com

Danielle M. Sloane
(615) 742-7763
dsloane@bassberry.com

Nesrin Garan Tift
(615) 742-7903
ntift@bassberry.com

Leigh Walton, Co-Chair
(615) 742-6201
lwalton@bassberry.com

Elizabeth S. Warren
(615) 742-7719
ewarren@bassberry.com

Douglas M. Wolford
(615) 742-7917
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.

315 Deaderick Street • Suite 2700 • Nashville, TN 37238-3001 • (615) 742-6200
The Tower at Peabody Place • 100 Peabody Place, Suite 900 • Memphis, TN 38103-3672 • (901) 543-5900
1700 Riverview Tower • 900 S. Gay Street • Knoxville, TN 37902 • (865) 521-6200