New HIPAA Regulations Require Notification of Breaches of Unsecured Protected Health Information

GEORGE CHORIATIS

In this article, the author discusses the new Health Insurance Portability and Accountability Act ("HIPAA") regulations which require a healthcare provider and other persons subject to HIPAA, upon discovering that any unsecured protected health information held by them has been used or disclosed in breach of certain privacy requirements of HIPAA, to notify the affected patients, U.S. Department of Health and Human Services, and, in the case of a breach involving at least 500 patients, the media.

On August 24, 2009, the U.S. Department of Health and Human Services ("HHS") published new regulations under the Health Insurance Portability and Accountability Act ("HIPAA"), which require a healthcare provider and other persons subject to HIPAA, upon discovering that any unsecured protected health information held by them has been used or disclosed in breach of certain privacy requirements of HIPAA, to notify the affected patients, HHS, and, in the case of a breach involving at least 500 patients, the media (the "Breach Notification Regulations").[1] The Breach Notification Regulations are applicable to breaches that occur on or after September 23, 2009.

The Breach Notification Regulations affect all HIPAA "covered entities." A covered entity is (i) a health plan, (ii) a health plan clearinghouse,

George Choriatis is an attorney in Rivkin Radler LLP's Corporate & Commercial and Health Services Practice groups. He may be contacted at george.choriatis@rivkin.com.

Published in the September 2009 issue of Privacy & Data Security Law Journal.

or (iii) a health care provider (including a physician, physician organization, hospital, skilled nursing facility, home health agency, etc.) which transmits in electronic form any protected health information in connection with the processing of claims for payment for health care services or any other financial or administrative transactions regulated by HIPAA.[2] The Breach Notification Regulations also affect "business associates" of covered entities, which include any person (other than an employee of the covered entity) who, on behalf of the covered entity, performs a function, activity, or service that involves the use or disclosure of protected health information.[3] Business associates include medical billing companies, medical transcription companies, professional service firms (such as law firms and accounting firms) that perform services involving the use of protected health information, and other such companies. It is important that covered entities and their business associates understand the Breach Notification Regulations, because there are certain actions that they can take now to minimize or even avoid potential liability under the Breach Notification Regulations, as discussed further below.

BACKGROUND

Since its enactment in 1996, HIPAA has prohibited covered entities from using or disclosing a patient's individually identifiable health information except either as HIPAA permits or requires or as the patient authorizes in writing. The Breach Notification Regulations stem from several significant amendments to HIPAA that were included in the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), which was enacted by the U.S. Congress on February 17, 2009 as part of the federal stimulus bill, the American Recovery and Reinvestment Act of 2009 (the "ARRA"). In brief, such amendments to HIPAA (i) impose additional requirements that must be satisfied by covered entities, (ii) make HIPAA directly applicable to persons other than covered entities, including business associates of covered entities, and (iii) strengthen HIPAA's enforcement provisions. Specifically, the Breach Notification Regulations are intended to implement the amendment contained in § 13402 of ARRA, which amended HIPAA to require covered entities and

their business associates, upon discovering that any of their unsecured protected health information has been acquired, accessed, used or disclosed in breach of certain privacy requirements of HIPAA, to provide notice of the breach to various persons. To carry out such amendment, the HITECH Act instructed HHS to promulgate regulations implementing the amendment,[4] and the Breach Notification Regulations were adopted by HHS pursuant to such instruction. The Breach Notification Regulations will be codified as a new Subpart D to part 164 of Title 45 of the Code of Federal Regulations ("CFR").

Prior to the enactment of the HITECH Act, a covered entity did not have an obligation to notify affected patients of any breaches of HIPAA. In brief, a covered entity, upon discovering that it had breached HIPAA, was required to mitigate, to the extent practicable, any harmful effect of the breach.[5] Although, under some circumstances, notice of the breach to the affected individuals might have been necessary to mitigate the harmful effects of the breach, such notice was by no means mandatory. Second, a covered entity was required to document the breach and to retain such documentation for at least six years.[6] Such requirement was imposed because HIPAA provides to a patient the right to request from a covered entity an accounting of all disclosures or uses of his or her protected health information by it during the six year period prior to the request for such accounting.[7] Third, the covered entity was required to sanction any employees responsible for the breach and adopt certain other safeguards.[8] The HITECH Act did not affect the foregoing obligations, and covered entities will continue to have such obligations. However, the HITECH Act and the Breach Notification Regulations adopted pursuant thereto have imposed on covered entities an additional obligation to provide notice to various persons in the event of certain breaches of HIPAA, as discussed below.

MAKING SENSE OF THE BREACH NOTIFICATION REGULATIONS

As discussed further below, the Breach Notification Regulations provide that, if a covered entity discovers after September 23, 2009 that any of its unsecured protected health information has been acquired, accessed, used, or disclosed in breach of certain privacy requirements of HIPAA,

then it must notify the affected individuals without unreasonable delay.[9] The covered entity also must notify HHS within 60 days of the end of the calendar year during which the breach occurred; however, if the breach involves the protected health information of at least 500 individuals, the covered entity must notify HHS at the same time that it notifies the affected individuals.[10] In addition, if the breach involves the protected health information of at least 500 individuals of a State or jurisdiction, the covered entity must notify prominent media outlets serving such State or jurisdiction.[11] Regardless of whether a breach occurs, a covered entity is required to train all members of its workforce with respect to the Breach Notification Regulations and to incorporate the new requirements in its HIPAA policies and procedures.[12] Pursuant to the HITECH Act, HHS will post on its website a list of covered entities that undergo breaches of unsecured protected health information involving at least 500 patients.

The Breach Notification Regulations also impose notification obligations on business associates.[13] Thus, if a business associate of a covered entity discovers after September 23, 2009 that any unsecured protected health information of the covered entity has been acquired, accessed, used, or disclosed in breach of certain requirements of HIPAA, then it is also required to send out a notice of the breach without unreasonable delay, but such notice must be sent to the covered entity instead of the affected individuals, HHS, or the media.[14] The covered entity, in turn, would then be obligated under the Breach Notification Regulations to send out the appropriate notices to the affected individuals, HHS, and the media.

An analysis of the Breach Notification Regulations necessarily entails a two-part inquiry. The first part of the inquiry focuses on the threshold issues that must be addressed under any given set of circumstances in order for a covered entity or business associate to determine whether it has an obligation to deliver any notices pursuant to the Breach Notification Regulations under such circumstances. Such threshold issues are discussed below. Once a covered entity or business associate determines that its obligation to deliver such notices has been triggered under a given set for circumstances, then the second part of the analysis would focus on the requirements relating to the notices that must be delivered. Such requirements are discussed below. The burden of proof applicable under the

Breach Notification Obligations is also discussed below. Finally, certain administrative safeguards that must be put in place regardless of whether or not a breach occurs are the subject of a section below.

The Threshold Issues

As discussed above, the general rule is that, (a) if a covered entity or business associate (i) discovers (ii) a breach of (iii) unsecured protected health information, then (b) it is required to notify various persons of the breach. Accordingly, to determine whether a covered entity or business associate has an obligation to deliver any notices under the Breach Notification Regulations, the following threshold questions must be answered:

- Did a *breach* occur? If not, then the notification obligations are not triggered. If the answer is "yes," then the next question is:
- Was the information that was the subject of the breach *unsecured protected health information*? If the breach related to secured protected health information and did not involve any unsecured protected health information, then the notification obligations are not triggered. However, if the breach did relate to unsecured protected health information, the third question is:
- Was the breach *discovered*? The notification obligations are triggered upon a "discovery" of a breach of unsecured personal information. Accordingly, the final threshold issue that must be addressed is determining the circumstances under which the covered entity or business associate will be treated as having discovered the breach.

The definitions of the highlighted terms are discussed below. In applying the above analysis to a given set of factual circumstances, it is helpful to consider the second question above (i.e. whether the information that was the subject of the breach was unsecured protected health information) first, before addressing the other two questions. Accordingly, the following discussion of the highlighted terms above begins with the definition of "unsecured personal health information" and then moves on to the definitions of the other highlighted terms.

How to Determine Whether Certain Information Is "Unsecured Protected Health Information"

"Unsecured protected health information" means protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS.[15] Accordingly, to determine whether certain information constitutes "unsecured protected health information," the following two-part inquiry must be undertaken:

- Is the information "protected health information?" If not, then the information does not fall within the definition of "unsecured protected health information." If the answer is "yes," then the next question is:
- Has such protected health information been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the HHS? If it has, then the information is not unsecured protected health information. If it has not, though, then the information is unsecured protected health information.

How to Determine Whether Information Is "Protected Health Information"

With respect to "protected health information," no change was made to the definition of such term by either the Breach Notification Regulations or the HITECH Act. In brief, "protected health information" refers to the individually identifiable health information of a patient, regardless of whether such information is stored electronically, on paper, or otherwise. Definitions of the term "protected health information," "individually identifiable information," and "health information" are contained in 45 CFR § 160.103.

How to Determine Whether Protected Health Information Is Unsecured

Protected health information may be rendered unusable unreadable, or indecipherable to unauthorized individuals through the use of a technol-

ogy or methodology specified by HHS in a written guidance prepared by it for such purpose. Such guidance was initially published by HHS in April, 2009, but HHS revised it in response to public comments it subsequently received, and the revised guidance was published together with the Breach Notification Guidelines on August 24, 2009.[16] Pursuant to the guidance, there are two ways that information may be rendered unusable unreadable, or indecipherable to unauthorized individuals — the information can be either (a) encrypted, if it is used in electronic form, or (b) destroyed, if it is used in either electronic form or paper form. Thus, encryption and destruction are the only two ways that protected health information may be rendered secure. If the protected health information is used in paper form, the only way to render it secure may be to destroy it.

Encryption. Information may be 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 process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt."[17] Valid encryption processes for "data at rest" (i.e. stored data that resides in databases, file systems, flash drives, memory, and any other structured storage method) are those encryption processes consistent with National Institute of Standards and Technology ("NIST') Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.[18] Valid encryption processes for "data in motion" (i.e. data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange are those which comply, as appropriate, with (a) the following NIST Special Publications: (i) 800-52, Guidelines for the Selection and Use of Transport Layer Security ("TLS") Implementations; (ii) 800-77, Guide to IPsec VPNs; or (iii) 800-113, Guide to SSL VPNs; or (b) any other standards that are Federal Information Processing Standards ("FIPS") 140-2 validated.[19]

Destruction. Information may be properly destroyed as follows: If the information is stored on paper, film, or other hard copy media, then

such information may be destroyed by shredding or destroying it such that the information cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction. If the information is stored electronically, the information can be destroyed if the electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization such that the information cannot be retrieved.[20]

How to Determine Whether a Breach Has Occurred

"Breach" is specially defined under the Breach Notification Regulations as (a) the acquisition, access, use, or disclosure of protected health information (b) in a manner not permitted under Subpart E of the "Privacy Rule" promulgated by HHS under HIPAA (such Subpart E is codified at 45 CFR 164.500 through 164.534), and (c) which compromises the security or privacy of the protected health information.[21] Moreover, the Breach Notification Regulations contains three exceptions to the foregoing definition for certain uses that are unintentional and certain disclosures that are made inadvertently or in good faith, as discussed further below.

Accordingly, to determine whether a "breach" has occurred, the following four part inquiry is useful:

Question No. 1: Has unsecured protected health information been acquired, accessed, used, or disclosed?

The terms "use" and "disclose" were previously defined in 45 CFR 160.103, and the Breach Notification Regulations make no changes to such definitions. "Use" means, with respect to protected health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information. "Disclosure" means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. HHS's preamble to the Breach Notification Regulations clarify that the terms "acquisition" and "access" are not specially defined and will be interpreted based on their plain meanings, and that, in any event, they are encompassed within the current definitions of "use" and "disclosure."

To avoid any inconsistencies, the Breach Notification Regulations revised the definition of the term "access" at 45 CFR 164.304 to clarify that the special meaning given to such term in that regulation is inapplicable to the Breach Notification Regulations.

If the answer to Question No. 1 above is "no," then a breach has not occurred. If the answer is "yes," then the next question is:

Question No. 2: Does such acquisition, access, use, or disclosure fall within any of the exceptions to the definition of breach, which are as follows:

(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 the HIPAA privacy rule;

(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 the HIPAA privacy rule; and

(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.

If the answer to Question No. 2 above is "yes," then a breach has not occurred. If the answer is "no," then the next question is:

Question No. 3: Does such acquisition, access, use, or disclosure violate any of the requirements of subpart E (codified at 45 CFR 164.500 through 164.534) of the HIPAA privacy rule?

We are now entering into the realm of HIPAA that has preoccupied HIPAA attorneys for years. By way of background, HIPAA consists of 42 U.S.C. § 1320d et seq. and the regulations promulgated by the Department of Health and Human Services thereunder, which are codified at 45 CFR parts 160, 162, and 164 (the "HIPAA Rules"). The basic substantive requirements of the HIPAA Rules are contained in the following subdivisions of the HIPAA Rules: (i) the HIPAA privacy rule (consisting of 45 CFR Part 160 and Subparts A and E of Part 164), which governs the use and disclosure of protected health information; and (ii) the HIPAA security rule (consisting of 45 CFR Part 164, Subparts A and C), which requires persons subject to HIPAA to adopt certain administrative, technical, and physical security safeguards to assure the confidentiality of protected health information. Not every violation of the HIPAA statute or the HIPAA Rules constitutes a "breach" for purposes of the Breach Notification Regulations. Only a violation of Subpart E of the privacy rule constitutes a "breach" that triggers an obligation to send the various notices pursuant to the Breach Notification Regulations. As a general matter, Subpart E of the privacy rule prohibits the use or disclosure of protected health information except either as permitted or required thereunder or as the patient authorizes in writing. Accordingly, only those violations of HIPAA which relate to the use or disclosure of protected health information will constitute a "breach" for purposes of the Breach Notification Regulations.

If the answer to Question No. 3 above is "no," then a breach has not occurred. If the answer is "yes," then the next question is:

Question No. 4: Does such violation "compromise the security or privacy of the protected health information?"

A violation compromises the security or privacy of the protected health information if it "poses a significant risk of financial, reputational, or other harm to the individual." HHS's preamble to the Breach Notification Regulations states that, to determine whether there is a "significant risk" of harm to an individual as a result of the violation, covered entities and business associates will need to perform a risk assessment.[22]

It also states that, in conducting such risk assessment, covered entities and business associates may consider the following factors: (i) whether the recipient of the information is obligated to protect the privacy and security of the information it received in the same or similar manner as the entity that disclosed the information; (ii) whether any steps taken by the covered entity immediately following the violation to mitigate an 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, eliminate or reduce the risk of harm to the individual to a less than "significant risk;" (iii) whether the impermissibly disclosed protected health information is returned prior to it being accessed for an improper purpose; and (iv) whether the nature of the protected health information poses a significant risk of financial, reputational, or other harm.[23] In addition, HHS's preamble to the Breach Notification Regulations state that a helpful discussion of additional factors that may appropriately be considered is contained in a memorandum of the U.S. Office of the Management and Budget intended for use by federal agencies, which contains guidelines regarding safeguarding against and responding to the breach of personally identifiable information in the possession of the agencies.[24]

If the answer to Question No. 4 above is "no," then a breach has not occurred. If the answer is "yes," then a breach has occurred.

How to Determine Whether and When a Breach Was Discovered

A covered entity will be treated as having "discovered" a breach on the first day that the breach is known to the covered entity or, by exercising reasonable diligence would have been known to it.[25] Moreover, knowledge of a breach will be ascribed to the covered entity if any person, other than the person committing the breach, who is a workforce member or agent of the covered entity, has knowledge of the breach or, by exercising reasonable diligence, would have had knowledge of the breach.[26] The term "workforce member" is specially defined in 45 CFR 160.103 as "employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the

direct control of such entity, whether or not they are paid by the covered entity." The term "agent" means any person who is deemed to be an agent of the covered entity under the federal common law of agency.[27] The term reasonable diligence" means the "business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances."[28]

Similarly, if a business associate commits a breach of unsecured protected health information, the business associate will be treated as having discovered the breach on the first day that the breach is known to it or, by exercising reasonable diligence, would have been known to it.[29] Knowledge of a breach will be ascribed to the business associate if any of its officers, employees or agents, other than the person committing the breach, has knowledge of the breach or, by exercising reasonable diligence, would have had knowledge of the breach.[30]

If a covered entity's business associate discovers that it has committed a breach of unsecured protected health information of the covered entity, then the covered entity will be deemed to have discovered such breach as well, even if the covered entity does not have actual knowledge of the breach. That is so because a covered entity's business associate is an agent of the covered entity. As discussed above, a covered entity will be treated as having discovered a breach on the first day that any of its agents discovers the breach or, by exercising reasonable diligence, would have had knowledge of the breach. Accordingly, a covered entity will be treated as having discovered a breach on the first day that its business associate discovers the breach or, by exercising reasonable diligence, would have had knowledge of the breach.

The Notification Obligations

Once a covered entity or business associate has analyzed the above threshold issues and determined that its obligation to deliver such notices has been triggered, the next step would be to identify who it is required to notify, what the contents of such notice must consist of, when such notice should be delivered, and how such notice should be delivered. In brief, those obligations can be summarized as follows:

In each breach of unsecured protected health information, a covered entity must send notice of the breach to each individual whose unsecured protected health information the covered entity either knows or reasonably believes was the subject of the breach.

In all circumstances, a covered entity must notify each individual whose unsecured protected health information has been accessed, acquired, used, or disclosed as a result of the breach.[31] Such notice must be given not only to those individuals whose information the covered entity actually knows was involved in the breach, but also those whose information the covered entity "reasonably believes" was involved.[32]

The notice must include, to the extent possible, the following information: (i) a brief description of what happened, including the date of the breach and the date of discovery of the breach; (ii) a description of the types of information that were involved in the breach; (iii) any steps individuals should take to protect themselves from potential harm resulting from the breach; (iv) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and (v) contact procedures for individuals to ask questions or learn additional information, which must include a toll-free telephone number, an email address, website, or postal address. The notice must be written in plain language.[33]

The notice must be sent without unreasonable delay, but not later than 60 days following the discovery of the breach.[34] HHS's preamble to the Breach Notification Regulations clarifies that "the time period for breach notification begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in this rule."[35] In connection with the foregoing, it should be noted that the Breach Notification Regulations provide that the notice may be provided in one or more mailings, as information is available.[36] HHS also clarified that the "60 days is an outer limit and therefore, in some cases, it may be an "unreasonable delay" to wait until the 60th day to provide notification. For example, if a covered entity has compiled the information necessary to provide notification to individuals on day 10 but waits until day 60 to send the notifications, it would constitute an unreasonable delay despite the fact that the covered

entity has provided notification within 60 days."[37]

The notice must be provided in the following manner:[38]

(a) The notice must be in writing.

(b) Unless the covered entity knows that the individual has died, the notice must be sent by first class mail to the individual at the last known address of the individual. Alternatively, if the individual had agreed to electronic notice and such agreement has not been withdrawn by him or her, the notice may be sent by electronic mail. If the individual is a minor or otherwise lacks legal capacity due to a physical or mental condition, notice to the parent or other person who is the personal representative of the individual is sufficient. If the covered entity does not have sufficient contact information or the contact information it has is out of date, it may send a substitute notice in a manner reasonably calculated to reach the individual. If there is insufficient or out of date contact information for less than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means. If there is insufficient or out of date contact information for 10 or more individuals, the substitute notice must be in the form of either a conspicuous posting for a period of 90 days on the home page of the covered entity's website or a conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and, in either case, the notice must include a toll-free phone number that remains active for at least 90 days where an individual can learn whether his or her information was included in the breach.

(c) If the covered entity knows that the individual has died and has the address of his or her next of kin or personal representative, then the notice must be sent by first class mail to such next of kin or personal representative. If the individual has died but the covered entity does not have the contact information of the deceased individual's next of kin or personal representative, it need not send any substitute notice to anyone.

(d) A covered entity may send out a separate notice, in addition to that required above, in any case deemed by the covered entity to require urgen-

cy because of possible imminent misuse of unsecured protected health information. Such notice may be given by telephone or other means.

With respect to each breach of unsecured protected health information, the covered entity must notify HHS, but the form and timing of such notice depends on the number of individuals whose protected health information was the subject of the breach.

With respect to each breach of unsecured protected health information, a covered entity must notify HHS as follows:[39] If the breach involves the information of less than 500 individuals, then the covered entity must maintain a log all such breaches and submit the log to HHS within 60 days of the end of the calendar year during which the breach occurred. If the breach involves the protected health information of at least 500 individuals, regardless of whether or not they reside in the same State or jurisdiction, the covered entity must notify HHS at the same time that it notifies the affected individuals. The foregoing notices must be provided in the manner instructed by HHS on its website. Although such instructions were not available at the time of this writing, they will be posted by HHS on its website in the near future.

If the breach involves more than 500 individuals who reside in the same State or jurisdiction, the covered entity must notify the media outlets serving such State or jurisdiction.

If the breach involves more than 500 individuals of a State or jurisdiction, the covered entity must notify prominent media outlets serving such State or jurisdiction.[40] The term "jurisdiction" refers to a geographic area smaller than a state, such as a county, city, or town. The term "prominent media outlet" was purposely left undefined in order to provide covered entities flexibility to select media outlets that are appropriate for the State or jurisdiction involved.

The obligation to send a notice to the media is triggered only if the 500 or more individuals affected reside in the same State or jurisdiction. If they do not, then there is no obligation to send a notice to the media. HHS included the following example in its preamble to the Breach Notification Regulations: "If a covered entity discovers a breach of 600 individuals,

200 of which reside in Virginia, 200 of which reside in Maryland, and 200 of which reside in the District of Columbia, such a breach did not affect more than 500 residents of any one State or jurisdiction, and as such, notification is not required to be provided to the media."[41]

Although the notice to the media is intended to be directed "to" the media and must be sent in addition to any notice that is sent to the affected individuals, it must contain the same information as that required to be given to the affected individuals. In addition, it must be given within the same time period as the notice required to be given to the affected individuals.

In each breach of unsecured protected health information by a business associate, the business associate must notify the covered entity.

A business associate who discovers a breach of unsecured personal health information does not have any obligation to notify the affected individuals, HHS, or the media.[42] Instead, it is required to notify the covered entity. Such notice must be given within 60 calendar days after the business associate discovers the breach. The notice must contain the following information: (i) to the extent possible, the identification of each individual whose information was, or is reasonably believed by the business associate to have been, the subject of the breach; and (ii) any other available information that the covered entity is required to include in its notification to the affected individual. Upon receiving the notice of breach from the business associate, the covered entity, in turn, would then be obligated under the Breach Notification Regulations to send out the appropriate notices to the affected individuals, HHS, and the media.

Covered entities and business associates should consider the impact of the foregoing notification obligations on their business associate agreements. By way of background, a covered entity is required under HIPAA to enter into a "business associate agreement" with each of its business associates to ensure that the business associate safeguards the confidentiality of the protected health information of the covered entity. At a minimum, HIPAA requires that a business associate agreement contain certain mandatory provisions pursuant to which the business associate shall agree to safeguard the covered entity's protected health information. However, a

well-drafted business associate agreement would also contain mechanisms — such as representations, warranties, and indemnities — which allocate between the covered entity and the business associate the foreseeable risks of liability and loss in the event that the business associate uses or discloses the protected health information in any manner that would constitute a violation of HIPAA by the covered entity. Covered entities and business associates should review their business associate agreements to ensure that the agreements appropriately address their respective obligations and risks in the event of a breach of unsecured protected health information by the business associate.

A covered entity and business associate is required to delay the giving of any notice upon the request of a law enforcement official if certain conditions are satisfied.

A covered entity and business associate is required to delay the giving of any notice if a law enforcement official states that a notice required under the Breach Notification Regulations would impede a criminal investigation or cause damage to national security.[43] If the statement is in writing and specifies the time for which a delay is required, then the covered entity or business associate need not take any further action until the end of the time period for which a delay is required. If the statement is made orally, the covered entity or business associate must document the statement, including the identity of the official making the statement, and delay the notice temporarily but not longer than 30 days from the date of the oral statement, unless during such period the law enforcement official submits a written statement specifying a longer period of time for which a delay is required.

The Breach Notification Regulations moved the definition of the term "law enforcement official" from 42 CFR 164.501 to 42 CFR 164.103, but they did not revise it in any manner. A "law enforcement official" means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Burden of Proof

In the event of an impermissible use or disclosure of protected health information, the burden of proof lies on the covered entity/ business associate to establish either that (i) it complied with the notification obligations or, alternatively, (ii) that the threshold requirements giving rise to the notification obligations were not met, and therefore, it was not obligated to send out any notices.[44] Due to the foregoing, HHS cautions that "when a covered entity or business associate knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment or the application of any exceptions to the definition of 'breach' to demonstrate that notification was not required."[45]

Administrative Obligations

HIPAA requires covered entities to adopt various administrative safeguards to protect the confidentiality of protected health information.[46] The Breach Notification Regulations require that covered entities review certain of these administrative safeguards, and, where necessary, incorporate into such administrative safeguards the new obligations imposed on them under the Breach Notification Regulations.[47] In brief, the administrative safeguards that need to be reviewed under the Breach Notification Obligations are those that require a covered entity to develop appropriate policies and procedures with respect to protected health information to assure compliance with HIPAA, to train its employees and other workforce members on such policies and procedures and sanction them for failure to comply with such policies and procedures, to provide a process for individuals to make complaints regarding a failure of the covered entity to comply with such policies and procedures, and to refrain from intimidating or retaliatory acts against a complainant.

ACTIONS THAT MAY BE TAKEN TO MINIMIZE LIABILITY UNDER THE BREACH NOTIFICATION OBLIGATIONS

Covered entities and their business associates may minimize or even

avoid any potential liability under the Breach Notification Regulations by taking the following actions:

Securing Protected Health Information

Covered entities and their business associates may avoid any potential liability under the Breach Notification Regulations as well as avoid the possibility of having to provide the required notices by taking steps now to secure any protected health information held by them. As discussed above, the notification obligations imposed by the Breach Notification Regulations are triggered only by breaches of *unsecured* protected health information. Indeed, HHS recognizes that many covered entities and business associates will voluntarily choose to secure their protected health information in order to avoid the possibility of having to provide breach notifications and it encourages them to take such an approach.

Adoption of Systems and Controls Appropriate for Detecting Breaches

As discussed above, a covered entity or business associate is liable under the new regulations for failing to provide a required notice in connection with a breach if the covered entity or business associate did not know of the breach, but, by exercising reasonable diligence, would have known of the breach. Accordingly, such entities should put in place systems and controls pursuant to which the appropriate persons within their organizations are made aware of any breaches, so that they can timely send the required notices.

Modification of HIPAA Policies and Procedures

As discussed above, covered entities will be in violation of the new regulations unless they revise their HIPAA policies and procedures to incorporate the additional obligations imposed on them under the new regulations. Accordingly, covered entities should not delay in doing so.

Amendment of Business Associate Agreements

As discussed above, covered entities and their business associates should ensure that their business associate agreements appropriately address their respective obligations in the event of a breach of unsecured protected health information by the business associate.

NOTES

[1] 72 F.R. 42740 (August 24, 2009).
[2] 45 CFR § 160.103.
[3] *Id*.
[4] *See* ARRA § 13402(j).
[5] 45 CFR § 164.530(f).
[6] 45 CFR § 164.528.
[7] 45 CFR 164.528.
[8] 45 CFR § 164.430.
[9] 45 CFR § 164.404(a).
[10] 45 CFR § 164.408.
[11] 45 CFR § 164.406.
[12] 45 CFR § 164.414.
[13] As briefly mentioned above, one of the more significant changes made by the HITECH Act to HIPAA was that it makes HIPAA directly applicable to business associates of covered entities. The Breach Notification Regulations are just one example of those provisions that have been made directly applicable to business associates. A discussion of such change, however, is beyond the scope of this article.
[14] 45 CFR § 164.410.
[15] 45 CFR § 164.402.
[16] 72 F.R. 42740, 42743.
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] 45 CFR § 164.402.
[22] 45 CFR § 164.404(a)(2).
[23] *Id*.

[24] *See* OMB Memorandum M-07-16, dated May 22, 2007, available at www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf.
[25] 45 CFR § 164.404(a)(2).
[26] *Id.*
[27] 72 F.R. 42740, 42749.
[28] *Id*.
[29] 45 CFR § 160.410.
[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] 45 CFR § 160.404(c).
[34] 45 CFR § 160.404(b).
[35] 72 F.R. 42740, 42744.
[36] 45 CFR § 160.404(d)(1).
[37] 72 F.R. 42740, 42744.
[38] 45 CFR § 160.404(d).
[39] 45 CFR § 160.408.
[40] 45 CFR § 160.406.
[41] 72 F.R. 42740, 42752.
[42] 45 CFR § 160.410.
[43] 45 CFR § 160.412.
[44] 45 CFR § 160.414(b).
[45] 72 F.R. 42740, 42755.
[46] *See* 45 CFR 164.530.
[47] *See* 45 CFR 164.414(a), which requires covered entities to incorporate the notification obligations into the administrative safeguards they have put in place pursuant to 45 CFR § 164.530(b), (d), (e), (g), (h), (i), and (j).