

2009 OCT 23 2009 10:46

RECEIVED - CMS
 OCT 23 2009
 2009
**COMMENTS OF THE AMERICAN CLINICAL LABORATORY
 ASSOCIATION ON THE BREACH NOTIFICATION FOR
 UNSECURED PROTECTED HEALTH INFORMATION
 INTERIM FINAL RULE
 (RIM 0991-AB56)**



American
 Clinical Laboratory
 Association

The American Clinical Laboratory Association (ACLA) is pleased to have this opportunity to submit our comments on the Breach Notification for Unsecured Protected Health Information Interim Final Rule (the "Interim Final Rule"). 74 *Fed. Reg.* 42740 (Aug. 24, 2009).¹ ACLA is an association representing clinical laboratories throughout the country, including local, regional, and national laboratories. As covered entities under the Health Insurance and Portability Act of 1996 (HIPAA), clinical laboratories will be directly affected by the Interim Final Rule. ACLA's comments will focus on the following issues: (1) the definition of "breach"; (2) notification of the individual; (3) notification of the Secretary; (4) notification by business associates; and (5) preemption of state law.

I. Definition of "Breach"

In the Interim Final Rule, the Department of Health and Human Services (HHS) defines "breach" as the "acquisition, access, use, or disclosure" of protected health information (PHI) in a manner that violates the HIPAA Privacy Rule and that compromises the privacy and security of the PHI.² Importantly, HHS includes a harm threshold in its definition of "breach" such that an unauthorized use or disclosure of PHI is considered a breach only if the use or disclosure poses a significant risk of harm to the individual. Additionally, there are three exceptions to the definition of "breach."

Given the importance of the breach definition as part of the new notification requirements, ACLA would like to express its comments with respect to certain elements of the definition. In particular, ACLA is commenting on the harm threshold that HHS has established for determining whether a breach has, in fact, occurred, and the enumerated exceptions.

A. Harm Threshold

ACLA supports HHS' decision to include a harm threshold in the definition of "breach" so that covered entities are not required to notify individuals each and every time there is an inadvertent use or disclosure of unsecured PHI. Despite having the appropriate HIPAA-compliant safeguards in place, PHI could still be inadvertently disclosed to, for example, a physician who is not the treating physician of the individual to whom the PHI belongs. Under such circumstances, little risk, if any, is posed to the individual as the recipient physician has a legal obligation to protect the privacy and security of the PHI. Therefore, it should be unnecessary for the covered entity to notify the patient of the inadvertent disclosure. If covered entities were required to notify a patient each time his or her PHI was inadvertently used or disclosed, individuals would potentially receive multiple notifications that could cause undue and unnecessary concern and alarm. Thus, ACLA

¹ The Interim Final Rule is available at <http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf>.

² *Id.* at 42767.

strongly favors the notion of a harm threshold to give covered entities the ability to determine whether a breach has, in fact, occurred. This interim step enables covered entities to ensure that individuals are only notified in the event that the incident would result in a significant risk of harm.

Notwithstanding ACLA's support of the harm threshold, however, ACLA is concerned that the risk assessment prescribed by HHS to determine whether the harm threshold is satisfied is overly vague and amorphous. For each situation where an individual's PHI is improperly or inadvertently used or disclosed, covered entities will be required to conduct an analysis to determine whether that use or disclosure poses a significant risk of harm to the individual and, therefore, constitutes a breach. Consequently, this analysis will be a key component to a covered entity's compliance with the breach notification requirements. If a risk assessment reveals that a breach did not occur then the covered entity would not be required to notify the individual. On the other hand, if the risk assessment reveals that a breach did occur the covered entity will be required to conduct a potentially costly and resource-intensive notification process.

Given then the importance of the risk assessment, HHS should provide more bright line guidance as to the way in which the risk assessment should be conducted by covered entities. Without such guidance, covered entities will carry out their own assessments on an ad hoc basis without a uniform threshold against which to measure the level of risk. As expected, this will result in some covered entities taking a more conservative approach in conducting their analyses and, thereby, require more frequent notification of individuals than the covered entities that elect to take a less conservative approach. This type of unlevel playing field will only penalize those covered entities that elect to be more conservative in an effort to comply with the regulation. Whereas, the less conservative covered entities may never determine that an improper use or disclosure rises to the level of a breach and may never find it necessary to notify an individual.

Accordingly, ACLA strongly encourages HHS to clarify the risk assessment that covered entities should conduct to determine whether an improper use or disclosure rises to the level of a breach. Specifically, at a minimum, HHS should define the term "significant risk," which is the standard against which covered entities are to determine whether a breach has occurred. In particular, with respect to the determination of whether a significant risk of financial harm exists, we urge HHS to identify specific data elements commonly found in State breach notification laws which, if contained in the PHI used or disclosed, would create a significant risk of financial harm (e.g., social security numbers or account numbers). HHS should also outline bright line factors for conducting a risk assessment. Further, HHS should specify "real-life" examples of situations that do and do not pose a significant risk to individuals using clear factors that the agency has enumerated. Again, by establishing clearer guidance with respect to the risk assessment process, covered entities will have a standard protocol for conducting their risk assessments. Additional clarity in this area will ensure that this important process will be one that all covered entities can apply uniformly in order to determine whether a breach has occurred.

B. Breach Exceptions

In light of the new burden that covered entities will face under the breach notification requirements, it is important that the exceptions to the definition of "breach" appropriately capture

the circumstances that should not be considered breaches under the regulation. First, as noted above, there are a number of “real life” situations that result in inadvertent uses or disclosures of a patient’s PHI that should not fall into the category of a breach and, therefore, should not warrant notifying the individual involved.

For example, one situation for clinical laboratories involves misdirected faxes. In the event of a misdirected fax, one covered entity may mistakenly fax a patient’s information to the wrong covered entity or business associate. While we recognize that covered entities should make every effort to ensure that such disclosures do not take place and should not be taken lightly, this type of inadvertent disclosure should not be considered a breach because the recipient covered entity or business associate, although an unauthorized recipient of the patient’s information, is subject to the same HIPAA regulatory safeguards as the covered entity that disclosed the information. In fact, in HHS’ brief discussion of factors that may be considered as part of a covered entity’s risk assessment, HHS states that an improper disclosure to another covered entity poses less risk to the individual because the recipient covered entity is obligated to protect the privacy and security of the information in a similar manner as the covered entity that disclosed the PHI. Given that HHS has already determined that inadvertent disclosures to other HIPAA covered entities pose little risk to the individual there is no reason then for the agency to require that covered entities conduct risk assessments each time such disclosures occur. Accordingly, inadvertent disclosures, such as misdirected faxes, to another covered entity or business associate should be excluded from the definition of “breach.” To ensure that such inadvertent disclosures are specifically included in the exceptions to the definition of “breach,” ACLA proposes that HHS modify the second breach exception as follows:

(2)(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to either another covered entity or business associate, or 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 is not further used or disclosed in a manner not permitted under subpart E of this part.³

This modification to the second exception will ensure that covered entities are not required to conduct a risk assessment every time a covered entity accidentally misdirects patient information to another covered entity or business associate. As acknowledged by HHS, this type of disclosure poses little risk to the individual and, therefore, should not be considered a breach as defined.

Second, with respect to the first and second breach exceptions, it is unclear how a covered entity will be able to determine whether the PHI will be further used or disclosed by the recipient entity in violation of the Privacy Rule. Specifically, how will the covered entity know whether the recipient further uses or discloses the PHI once the PHI has been unintentionally or inadvertently used or disclosed? Will the covered entity be responsible for any additional breaches of the PHI if it is further used or disclosed in violation of the Privacy Rule? HHS should provide guidance

³ ACLA is proposing additional changes to this second exception, which are discussed later in our comments.

regarding how a covered entity can determine whether the recipient has further used or disclosed PHI. In lieu of providing such guidance, ACLA requests that HHS remove from these exceptions the language that relates to further use or disclosure of the PHI. ACLA proposes that HHS modify these exceptions as follows:

(2)(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.~~

(2)(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to either another covered entity or business associate, or 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 is not further used or disclosed in a manner not permitted under subpart E of this part.~~

If HHS is unwilling to make the above modifications, in the alternative, HHS should hold covered entities harmless in the event that the entity makes a reasonable attempt to obtain from the recipient some form of communication indicating that the recipient would not further use or disclose the PHI and has destroyed the information. For example, placing unintended recipients on notice that they should destroy the information and that further use or disclosure of the information is prohibited by law, and requesting a reply to confirm destruction of the information and that it will not be further used or disclosed, should be considered sufficient means to mitigate the incident. Because obtaining these assurances from a recipient entity will be difficult, and in some cases impossible, such a hold harmless provision would ensure that covered entities that either receive or reasonably attempt to receive such assurances are not deemed responsible for any further breaches for which they are unaware.

Finally, HHS' use of the term "good faith" in its third exception to the definition of "breach" should be clarified. It is unclear from HHS' discussion as to how covered entities are to have a "good faith" belief that the PHI, once disclosed, could not reasonably be retained by the unauthorized recipient. Therefore, HHS should either provide additional guidance and clarity relating to this exception or provide some type of hold harmless provision to ensure that covered entities are not responsible for the actions of the unauthorized recipient. The covered entity should not be responsible for any further breaches of the PHI by the recipient if the PHI is retained by that recipient. As such, ACLA proposes the following modification to the third exception:

(2)(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 or the covered entity or business associate is notified by the unauthorized person that the PHI has been destroyed.

Short of making this modification to the exception, HHS should provide additional guidance to covered entities to clarify its meaning of "good faith" as used in this exception.

II. Notification of Individual

The Interim Final Rule requires that following the discovery of a breach of unsecured PHI, a covered entity notify each harmed individual whose PHI is involved in the breach. ACLA has concerns with respect to the content and methods of such notification. We have discussed those comments in turn below.

A. Content of Notification

HHS sets forth the content requirements for notifying individuals whose unsecured PHI has been breached. One of those requirements directs that covered entities include in their notification the steps that individuals should take to protect themselves from potential harm resulting from the breach. While ACLA supports the rationale behind requiring that such information be included in notification to the individual, we are concerned that providing such information may result in liability on the part of the covered entity if the covered entity were to provide information to the harmed individual that proved to be incorrect or inaccurate. Additionally, there may be information that a covered entity has a duty to provide an individual with respect to a breach of medical information with which the covered entity may not be aware. Unlike data breaches involving financial institutions, where individuals know to contact their financial institutions and the credit bureaus, breaches of PHI are not currently associated with commonly known and accepted steps for individuals to use or for covered entities to turn to assist individuals. For example, how would a covered entity advise an affected individual regarding mitigation of a reputational harm if PHI is inadvertently used or disclosed? As such, covered entities could be potentially exposed to undue liability in the event that harmed individuals sought action against the covered entities based on their efforts to comply with their notification requirement.

Accordingly, ACLA recommends that HHS provide that covered entities will be held harmless in the event that the notified individual has a claim or demand against the covered entity as a result of the information provided, or not provided, to the individual, where the covered entity has notified the individual of steps that the individual should take to protect himself or herself from potential harm resulting from the breach. In fact, HHS should make clear that there will be instances where there will be no steps for individuals to take to protect themselves from the breach and, therefore, nothing for covered entities to provide. In lieu of such protections for covered entities, ACLA strongly encourages HHS to provide further guidance that sets forth clear parameters as to the information that a covered entity should make available to harmed individuals as part of the notification requirement. Specifically, HHS should post on the agency's website the appropriate information that covered entities should provide to individuals to comply with this requirement. As an alternative to posting information on the agency's website, HHS should direct covered entities to endorsed sources of information, such as the American Health Information

Management Association (AHIMA), that covered entities can look to in providing the necessary information to harmed individuals in the event of a breach of their PHI. It would be helpful for covered entities to know whether materials from organizations, such as AHIMA, which have developed guidance on what individuals should do in the event of a security breach or potential medical identity theft, would be sufficient in order for covered entities to comply with this component of the breach notification requirements. Providing such guidance will ensure that harmed individuals are given accurate and consistent instructions as to the ways in which they can protect themselves from potential harm following a breach of their PHI.

B. Method of Notification

The method for notifying individuals of a breach of their unsecured PHI is predicated on the assumption that covered entities have access to, and maintain, contact information for the individuals to whom they provide services. However, while this may be true for covered entities that are direct treatment providers, such as physicians and hospitals, this is not the case for clinical laboratories. Unlike physicians and hospitals, in a significant number of cases clinical laboratories do not have face-to-face interactions with the individuals to whom they provide services and, therefore, there is often no opportunity to obtain the necessary contact information (*e.g.*, phone numbers and addresses) to reach individuals directly. In fact, reference laboratories are many times removed from the patient and will be unlikely to have the necessary information to contact individuals. Instead, as indirect treatment providers, clinical laboratories rely on other covered entities, such as physicians and hospitals, to obtain and provide such information, and it is often lacking even when requested. Thus, for indirect treatment providers, such as clinical laboratories, HHS should provide guidance as to what recourse covered entities will have if they do not have or are simply unable to obtain the contact information necessary to notify the individual.

Given that clinical laboratories often will not have the information necessary to be able to provide written notice to harmed individuals by first class mail in the event of a breach, clinical laboratories will likely have to rely primarily on the substitute notice to individuals. However, HHS offers little guidance as to how a covered entity should provide such notice that contains the same elements as the written notice in a manner that reaches impacted individuals without further breaching their PHI. Practically speaking, it will be extremely difficult for covered entities to provide the required notice in a manner calculated to reach certain individuals without disclosing some level of specificity regarding the breach on the covered entity's website or in the media. While HHS cautions that covered entities should be mindful of unnecessarily disclosing the individual's PHI when providing substitute notice, the agency fails to instruct covered entities as to how, in fact, to accomplish this effectively. As such, HHS should bring additional clarification to this issue of how covered entities should provide substitute notice through using their websites or the media without further disclosing the individual's PHI.

Additionally, ACLA urges HHS to require that covered entities make only a reasonable attempt to contact harmed individuals when substitute notice is required. With respect to substitute notice for fewer than 10 individuals, HHS should only require that the covered entity make a reasonable attempt (*e.g.*, attempting to obtain contact information from the treating physician) to contact the harmed individuals through substitute means. Following such reasonable attempt, HHS

should make clear that the covered entity may cease any further attempts. For substitute notice involving 10 or more individuals, HHS should make clear that the 90-day posting on the covered entity's website or in the media would be considered to be a reasonable attempt to contact the harmed individuals. Following such reasonable attempt, the covered entity may cease any further attempts to notify individuals. Requiring that covered entities make only a reasonable attempt to contact individuals will ensure that covered entities are not using unlimited resources to attempt to contact individuals indefinitely.

III. Notification of Secretary

In accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act, covered entities are required to notify the Secretary of breaches of unsecured PHI.⁴ For breaches involving 500 or more individuals, covered entities are required to notify the Secretary immediately. For breaches involving less than 500 individuals, the covered entity is required to notify the Secretary on an annual basis by maintaining a log of such breaches. The language that the covered entity should maintain a log is set forth in both the HITECH Act and the agency's proposed regulatory language (42 C.F.R. §164.498). However, HHS has recently posted on its website a form for covered entities to complete for each breach, regardless of whether more or less than 500 individuals are involved.

For breaches involving fewer than 500 individuals, HHS' posted form is inconsistent with the language set forth by Congress in the statute and the agency's own proposed regulatory language. Additionally, the completion of such a form will pose a significant burden on covered entities – a burden that was intended to be avoided by requiring the maintenance of a log under the statute. HHS, itself, acknowledges that the completion of the form will take between 15 and 30 minutes. Because HHS is compelled to comply with the underlying statutory language, and given the additional resources that covered entities will be required to expend to complete the form, HHS should require that covered entities only maintain a log of breaches and provide that log on an annual basis to the Secretary. ACLA strongly believes that requiring such a log is consistent with the language and intent of the statute.

IV. Notification by Business Associate

Business associates are required to notify covered entities of any breaches of unsecured PHI. Upon notification from the business associate, the covered entity is then responsible for notifying the harmed individual. However, for covered entities, the reliance on business associates to provide notification of any breaches that the business associate has or should have discovered is problematic for a number of reasons. First, it is particularly troubling that in the event that a business associate is acting as an agent of a covered entity, the business associate's discovery of a breach will be imputed to the covered entity. In instances where the business associate discovers a breach, how is the covered entity to ensure that the business associate notifies the covered entity in a timely manner to allow the covered entity to then comply with its obligations under the breach notification requirements? Although HHS suggests that covered entities may wish to include the timing of

⁴ See American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, § 13402(e)(3).

when the business associate should notify the covered entity in its business associate agreements to address this concern, there is still no guarantee that the business associate will comply with any timeline set forth in the agreement. If, for example, a business associate, in violation of its business associate agreement, notifies the covered entity on day 58 following the discovery of a breach, it will be impossible for the covered entity to comply with its risk assessment and notification requirements by day 60, and the covered entity will be exposed to penalties for non-compliance despite exercising its best efforts to ensure timely notification through contractual obligations imposed on its business associate.

In such instances, the covered entity should not be considered at fault for its inability to comply with the breach notification requirements. However, HHS is silent on this point, which could imply that HHS intends both the business associate and covered entity to be jointly and severally liable. This of course would be an unfair and unjustifiable outcome given that covered entities are in the tenuous position of having to rely on a business associate's diligence in discovering breaches and their ability to notify the covered entity within the appropriate timeframes established by the covered entity. As such, ACLA urges HHS to make clear that the business associate's discovery of a breach will not be imputed to the covered entity. Instead, HHS should make clear that once the business associate notifies the covered entity of a breach, the 60-day timeline begins upon such notification from the business associate, and not upon the business associate's discovery. If the business associate fails to notify the covered entity within 60 days, any liability attached to not complying with the breach notification requirements should rest solely with the business associate. This treatment of business associates is consistent with the expansion of the HIPAA Privacy and Security Rules to business associates under the HITECH Act.⁵ As set forth in those provisions of the HITECH Act, business associates will be held to many of the same standards as are covered entities with respect to the Privacy and Security Rules and the applicable penalties under each.

Second, business associates are required to provide covered entities, to the extent possible, the identity of the individuals whose unsecured PHI has been breached and any other available information that the covered entity is required to include in its notification. However, HHS is silent as to any recourse, or liability, that a covered entity may have if the business associate is unable or unwilling to provide the necessary information to allow the covered entity to notify the individual. Again, as we have expressed above, HHS should not hold covered entities accountable for that which is in the control of the business associate. If a breach is the fault of the business associate and the business associate cannot provide the necessary information to the covered entity, the covered entity should not be held responsible for violating the breach notification requirements. Instead, HHS should hold the business associate accountable for failing to comply with its notification requirements under the regulation. Accordingly, ACLA requests that HHS provide guidance addressing circumstances where the business associate is unable or unwilling to provide the information necessary for the covered entity to comply with its own requirements and hold business associates more accountable with respect to these requirements.

⁵ See ARRA §§ 13401, 13404.

Lastly, HHS suggests that the business associate and covered entity will continue to have flexibility to set forth obligations for each party in their business associate agreements.⁶ However, HHS leaves open the question as to whether a covered entity will be able to delegate its breach notification duties to its business associate. While the regulatory language clearly requires that the covered entity notify the individual (and the Secretary), HHS' discussion of the flexibility that business associates and covered entities will have with respect to determining who will provide notice seems contrary to the notification requirements imposed on covered entities by regulation. Thus, ACLA asks HHS to make clear whether a covered entity may delegate its duty to notify to its business associate in accordance with a business associate agreement. If, in fact, a covered entity is permitted to delegate its duty to notify to its business associate, ACLA asks HHS to make clear that the covered entity would then be relieved from its duty to notify under the breach notification requirements (including both notification to the individual and to the Secretary) in accordance with its contractual arrangement with the business associate.

V. Preemption

HHS provides that state law that is contrary to the federal breach notification requirements will be preempted. HHS specifies that state law is "contrary" when it is impossible to comply with both state and federal requirements. ACLA would like to express its support of the Interim Final Rule's preemption of state law. ACLA encourages HHS to maintain state preemption to ensure that covered entities are not required to comply with both state and federal breach notification requirements in the event that the state law is contrary to the federal requirements.

Thank you for the opportunity to comment. If you have any questions or need any further information, please do not hesitate to contact us.

⁶ See 74 *Fed. Reg.* at 42754.