American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

October 23, 2009

Kathleen Sebelius, Secretary
U.S. Department of Health and Human Service
Office for Civil Rights
Attention: HITECH Breach Notification
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, D.C. 20201

***Re: RIN 0991-AB56; Breach Notification for Unsecured Protected Health Information; Interim Final Rule, 74 Fed. Reg. 42740 (August 24, 2009).***

Dear Secretary Sebelius:

On behalf of our more than 5,000 member hospitals, health systems and other health care organizations, and our 40,000 individual members, the American Hospital Association (AHA) appreciates the opportunity to comment on the Department of Health and Human Services' (HHS) interim final rule on Breach Notification for Unsecured Protected Health Information published in the August 24 *Federal Register*. This rule implements the requirements from the *Health Information Technology for Economic and Clinical Health (HITECH) Act* for hospitals and other Health Insurance Portability and Accountability Act (HIPAA) covered entities and their business associates to notify individuals when a breach of their unsecured personal health information occurs.

America's hospitals are dedicated to safeguarding the privacy of their patients' medical information, and the AHA and its members support HHS' efforts to create a federal data breach notification requirement. We generally endorse the provisions of the interim final rule, particularly HHS' recognition that the federal breach requirements necessitate an explicit risk of harm trigger for the notice obligations. However, further improvements are needed to ensure the rule effectively serves its purpose with respect to the breach notification requirements under HITECH. We also have several recommendations about the breach notification provisions generally. Specifically, we urge HHS to:

- Identify additional situations where the department considers the privacy or security of information not to be compromised and, therefore, would not trigger the obligation to provide notice under the breach notification regulations;

- Rescind its guidance that a covered entity must determine whether each of its business associates is an agent to understand when knowledge of that business associate's breach will be imputed directly to the covered entity; and
- Create a process by which covered entities may submit electronically via the Internet a single annual log to notify HHS of breaches affecting fewer than 500 people.

**Risk of harm standard must be maintained in the final rule's definition of breach**
We greatly appreciate HHS' recognition of a risk of harm standard in the interim final regulations and strongly urge HHS to retain the interim final rule's definition of "breach" and its risk of harm trigger for the federal notice obligations in the final rule. HHS' implementation of the definition of "breach" is consistent with the statutory language of the HITECH Act, as well as with state laws and federal agency policies. It also is critical from a policy perspective.

In section 13400 of HITECH, Congress expressly defined "breach" as "the unauthorized acquisition, access, use, or disclosure of protected health information which *compromises the security or privacy of such information . . .*"(emphasis added). This language contemplates the need for some determination of whether there is a risk of harm to an individual before a breach has occurred. An acquisition, access, use or disclosure that does not compromise the security or privacy of the information is not a breach. The implementation of a risk of harm trigger in the rule's definition of "breach" is consistent with the statutory language relating to breaches of protected health information (PHI).

A majority of state breach notification laws provide that an incident is not a breach for which notice is required if there is no reasonable likelihood of harm (e.g., the likelihood of identity theft). As HHS notes, a risk of harm standard in the federal breach notification rule better aligns the federal breach notification requirements with state law requirements and existing obligations on federal agencies required to implement breach notification policies in compliance with OMB Memorandum M-07-16 (*See* 74 *Fed. Reg.* 42744). The OMB Memorandum, along with HHS' discussion in the rule's preamble, provides useful guidance to covered entities in establishing policies and procedures for identifying breaches and documenting their risk assessments.

We also note that a risk of harm standard is important from a policy perspective. The purpose of notifying individuals when their PHI has been the subject of a breach is to inform them to take certain precautions to mitigate harm. Notifying individuals of an unauthorized acquisition, access or disclosure of their PHI serves no useful purpose when a covered entity, through investigation, has determined that there is no reasonable likelihood of harm to the individuals. Instead, a breach notice in this circumstance would create unnecessary anxiety and concern among the individuals who would receive such notices. It also would create an unnecessary and unproductive administrative burden and expense for the covered entity.

We believe that it is critical to the successful implementation of a federal breach notification policy that patients be notified of breaches that pose a significant risk of harm, yet not receive countless notices of breaches that do not pose such harm. **Therefore, we strongly encourage HHS to maintain its definition of "breach" in finalizing this rule**.

**Rule's provisions create practical approach to incentivize use of limited data sets**
The AHA appreciates HHS' interpretation that a use or disclosure of PHI in the form of a restricted limited data set, with date of birth and zip code removed as well, does not compromise the privacy or security of the protected health information and as such does not trigger breach notification obligations (*See* 45 C.F.R. § 164.402). In combination with a risk of harm analysis for full limited data sets (i.e., those that do contain date of birth and/or zip code), HHS' interpretation creates a practical approach that will encourage the use of such data for research and public health purposes. Further, the AHA supports HHS' clarification at 74 *Fed. Reg.* 42746 that when a breach is caused by a third party to whom a covered entity or business associate has permissibly disclosed a limited data set, such entities will not be held responsible for such breaches, nor will the disclosing entities be subject to data breach notification requirements. We commend HHS for implementing the regulations in a way that is workable, does not disincentivize the creation and use of limited data sets, and therefore avoids a chilling effect on clinical and quality improvement studies.

**HHS should identify other situations in which a use or disclosure does not compromise privacy or security of PHI**
As noted above, the AHA supports HHS' classification of information from which limited data set identifiers, zip code and birth date are removed as data for which privacy or security is not compromised for purposes of a breach analysis. We urge the department to consider identifying additional situations in which the privacy or security of information is not considered compromised in the context of the breach notification regulations. For example, there are many conceivable situations in which inadvertent disclosures from one covered entity to another would not compromise the privacy or security of the information, such as where a hospital sends information to the wrong physician practice, mistakenly and in good faith. In this circumstance, both the disclosing and the receiving entities already are bound by the HIPAA privacy rule's obligation at 45 CFR § 164.530(f) to mitigate harm. We urge HHS to establish a category of disclosures like the one described above for which the privacy or security of the information would not be considered compromised. Such a category could be defined to apply only when the entities meet the privacy rule's obligations to mitigate harm or undertake steps mandated by HHS, such as returning the mistakenly disclosed information.

We suggest that a similar approach would be appropriate for uses and disclosures in which the only potential breach is the use or disclosure of more than the minimum necessary amount of information. While HHS stated in the preamble to the interim final rule at 74 *Fed. Reg*. 42744 that uses or disclosures of PHI that involve more than the minimum necessary information may qualify as breaches, we instead would suggest that it is not clear that these uses and disclosures are likely to impose a significant risk of harm. In part, this is because most "use" violations of the minimum necessary standard would occur within a covered entity or business associate, and the HIPAA privacy regulations at 45 CFR § 164.530(f) already obligate covered entities to take steps to mitigate harm in such circumstances. Congress and HHS have recognized this basic premise in enacting and implementing HITECH's statutory exceptions to the definition of breach, which exempt certain internal uses and disclosures from the breach notification requirements. We suggest that otherwise permissible uses that exceed the minimum necessary requirements

also would be appropriate for a category of information for which the privacy or security is not likely compromised.

While many uses in excess of the minimum necessary rule may be captured adequately under the breach exceptions, permissible disclosures in which the information disclosed is beyond the minimum necessary may not fall within the breach exceptions where the disclosure is from one covered entity to another covered entity. Again, we note that the HIPAA privacy regulations require covered entities to mitigate harm in such situations. It is unclear what benefit individuals gain from receiving notification of these circumstances. For example, consider a situation in which a hospital discloses more than the minimum necessary amount of a patient's information to the patient's health plan as part of a routine and permissible billing interaction; the hospital becomes aware of the problem and attempts to mitigate any harm. Without clarification from HHS that this type of situation does not compromise the privacy or security of the information, the hospital must bear the administrative cost of conducting a risk assessment, yet the benefit to the patient in receiving a breach notification in such a situation is murky.

**Rule appropriately implements statutory exceptions to breach definition**
The AHA commends HHS for implementing HITECH's statutory exceptions to the "breach" definition in a way that acknowledges and is consistent with the HIPAA privacy and security rules' requirements for covered entities and their business associates. We appreciate that HHS interpreted these exceptions in a way that does not unnecessarily require breach notification for internal uses and disclosures, an approach that provides direct benefits to patients without unnecessarily risking their care.

With respect to the breach definition exception for unintentional acquisition, access or use of protected health information included in the statute at 45 C.F.R. § 164.402(2)(i), we appreciate that HHS has applied this exception to "workforce members." *See* 74 *Fed. Reg.* 42747. Further, the AHA supports HHS' interpretation of the exception found in the statute at 45 C.F.R. § 164.402(2)(ii) to cover inadvertent disclosures of protected health information from a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at that same covered entity, business associate or organized health care arrangement (OHCA) in which the covered entity participates. Both interpretations promote workable compliance with privacy and security requirements while allowing health care entities to use PHI for routine internal purposes that enable and enhance quality patient care.

The AHA also appreciates HHS' clarification that the exceptions set forth in §164.402(2)(i) and (ii) apply only when there is no further unauthorized acquisition or disclosure of PHI. These exceptions cover unintentional acquisition, access or use of PHI by an employee or individual acting under a covered entity's or business associate's authority, when that acquisition, access or use was made in good faith and within the course of that employee's or individual's employment or professional relationship with the covered entity or business associate and the PHI is not further acquired, accessed, used or disclosed by any person. We strongly support HHS' interpretation of the exception as encompassing situations in which a recipient does not further use or disclose the information in a manner not permitted under the HIPAA privacy rule (*See* 74 *Fed. Reg.* 42747), meaning that the breach notification requirements will not apply when any

further acquisition, access, use or disclosure is authorized. These interpretations help ensure efficient and effective application of the breach notification rule.

Finally, the AHA commends HHS for clarifying that, for purposes of HITECH's statutory breach definition exception in section 13400(1)(B)(ii) and (iii) for inadvertent disclosures by a person who is otherwise authorized to access PHI at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility, "same facility" means the same legal entity or status of entities as an OHCA, rather than the same physical structure. This interpretation promotes ease of workability and provides practical benefits to covered entities, business associates and OHCAs that operate in and transmit information between numerous physical locations.

**Covered entities should not be required to determine agency status of their business associates**

The AHA is concerned by HHS' guidance at 74 *Fed.Reg.* 42754 that a covered entity's business associate may sometimes be an agent of the covered entity, and, in that case, the business associate's knowledge of a breach will be imputed to the covered entity for purposes of establishing when the covered entity learned of the breach. Federal common law on agency requires a detailed facts and circumstances analysis that easily could lead to differing conclusions depending upon who is engaging in the analysis.

The Restatement of Agency, a legal treatise on agency law, states that an entity is an agent only in narrow circumstances. For example, if the entity is acting on behalf of another entity and in the other entity's interest above the entity's own interest, and the entity has a fiduciary obligation to the other entity, it is an agent rather than an independent contractor. This fact-specific determination must be performed for each potential agency relationship. For a covered entity with thousands of business associates, this analysis would be an unquantifiable burden.

The AHA contends that abiding by the federal common law's fact-specific determination of agency is not a workable process by which to determine whether a business associate is a covered entity's agent. We strongly suggest that HHS clarify that all business associates are governed by 45 C.F.R. § 164.410(a), which details when a business associate must notify a covered entity of a breach, and that a covered entity will only "discover" a breach when informed of the breach by its business associate consistent with this timing requirement. Applying a uniform policy would prevent confusion and administrative burdens that would arise under a required fact-specific determination. In the alternative, if HHS believes that an agent distinction is necessary, HHS could limit its definition of agency to certain common fiduciary relationships, such as lawyer-client and accountant-client relationships.

It is crucial to note that the HIPAA enforcement rule does not require an agency determination for business associates for enforcement and liability purposes. In its place, the enforcement rule includes a business associate exception to the liability rules. If a covered entity meets all of HIPAA's business associate requirements, the covered entity does not have to make agency determinations with regard to its business associates. We strongly suggest that HHS utilize a similar approach in its breach notification regulations.

In sum, requiring agency determinations for each of a covered entity's business associates would create a substantial administrative burden for the covered entity. It would not be feasible for covered entities with thousands of business associates to engage in this determination for each business associate. Moreover, an agency determination requirement is inconsistent with HHS' approach to business associate relationships generally. We urge HHS to rescind its guidance that a covered entity should determine whether each of its business associates is an agent before determining when knowledge of that business associate's breach was imputed to the covered entity.

**HHS should create a process for submission of a single annual log of certain breaches**
The AHA supports the implementation of a uniform date for submission to HHS of annual logs of breaches affecting fewer than 500 people. We endorse HHS' requirement that these logs be submitted within 60 days after the end of each calendar year. We believe that establishing a single annual designated submission date will reduce potential confusion and make compliance easier and more efficient for the entities required to submit such logs. However, we note that the form for the submission of the annual logs, as posted on the HHS Web site, does not appear to contemplate the submission of an annual log, and we urge HHS to create a process by which covered entities may submit a single annual log.

**State law preemption clarification eliminates unnecessary anxiety and confusion of multiple breach notifications**
We appreciate HHS' explanation that the breach notification regulations will preempt conflicting state law. The AHA also commends HHS' clarification that notifications required by the federal breach notification law and regulations also may include information in addition to the information required under federal law. By clarifying this point, HHS allows entities to satisfy both federal and state requirements in one communication to affected individuals. This eliminates the anxiety and confusion that could arise when individuals receive multiple letters about the same breach but mistakenly believe that there has been more than one breach of their information.

In conclusion, HHS has taken important steps toward ensuring that the breach notification requirements provide for effective individual notification about any breach of PHI that creates a significant risk of harm to affected individuals while simultaneously being workable for providers who must comply with the rule's requirements. We believe that HHS can further improve the value of the rule for both patients and providers by making the additional refinements we recommend. If you have any questions about our recommendations, please contact Lawrence Hughes, assistant general counsel, at lhughes@aha.org or (202) 626-2346.

Sincerely,

Rick Pollack
Executive Vice President