



American Hospital
Association

HOSPITAL HIGHLIGHTS

Prepared for AHA members whenever there is important HIPAA-related news.
(If you do not receive five (5) pages of this document, call (202) 626-2973.)

HHS Releases Proposed HIPAA Enforcement Rule

April 27, 2005

The Department of Health and Human Services (HHS) published in the April 18, 2005 *Federal Register* proposed enforcement regulations (Enforcement Rule) for the administrative simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This Enforcement Rule would amend and supplement interim final enforcement regulations that were published in April 2003.

The American Hospital Association (AHA) is pleased with some changes proposed in the Enforcement Rule, but a number of significant areas of concern remain. HHS is accepting comments on the proposed rule until June 17, 2005, and the AHA urges hospitals to consider submitting comments about these regulations. A [copy of the Enforcement Rule](#) is available on the AHA's HIPAA Web site at www.aha.org.

Overview of the New Proposed Rule

The Enforcement Rule would apply to all HIPAA administrative simplification regulations – privacy, security, transactions standards, code sets, and identifiers. HHS reiterates its commitment “to promoting and encouraging voluntary compliance with the HIPAA rules through education, cooperation, and technical assistance.” But the rule concerns the procedural processes for imposing civil money penalties (CMPs) for a violation, including substantive detail about the basis of liability and the determination of CMP amounts. The rule does not address imposing criminal penalties for a HIPAA violation because these penalties are enforced by the Department of Justice.

Results from Prior Rulemaking

The Enforcement Rule includes several changes that the AHA recommended in its comments on the 2003 interim enforcement regulations. The [AHA's comments](#) on the interim rule can be found at www.aha.org. In response to the AHA's comments, HHS proposes amending the requirements for a notice of proposed determination - the notice alerts a covered entity that HHS believes it should be penalized for a HIPAA violation. The proposal would require the notice to provide information regarding the circumstances considered when determining the amount of the proposed penalty. The AHA is pleased that HHS has responded to its recommendations and incorporated this additional element into the notice to give hospitals more information regarding the penalty assessed.

HHS also responded to the AHA's concerns about covered entities' liability for the conduct of business associates by providing explicit assurance that covered entities are not liable for the acts of their business associates *so long as they take certain actions* required by the HIPAA Privacy Rule.

Finally, HHS clarifies and confirms that the administrative law judge (ALJ) may issue findings of fact and conclusions of law and, thus, may determine that no violation has occurred. The interim final enforcement regulations permit the ALJ to “affirm, increase or reduce the penalties imposed by the Secretary.” The AHA was concerned and told HHS that this language suggested that the ALJ may not be able to determine that there was in fact no violation. The AHA is pleased that in the new proposed rule an ALJ has the authority to evaluate whether there was a violation in the first place.

The AHA is extremely disappointed that HHS has maintained the interim regulations’ standard requiring that hospitals file a request for a hearing within 60 days of receiving a notice of proposed determination. The interim regulations require a hospital to include in the hearing request an admission, denial or explanation of the findings of fact contained in the notice, any defenses the hospital has, and the hospital’s legal and factual basis for opposing the penalty. In its comments on the interim regulation, the AHA made it clear that, in order to ensure hospitals appropriate due process and time to investigate and develop their defenses and explanations, HHS must either extend the time limit for requesting a hearing or permit less specificity in the request. HHS responded by asserting that, in HHS’ view, the hospitals will be aware of HHS’ investigation and details of the alleged violation long before receiving a notice of proposed determination and, thus, should have sufficient time to conduct an internal investigation and develop appropriate defenses.

The AHA also is very concerned about a number of additional proposals in the Enforcement Rule that could impose significant costs as a result of hospitals’ obligations to defend themselves. Hospitals will want to review these new procedures with their litigation risk management counsel and submit comments. The Enforcement Rule provisions most relevant for hospitals are highlighted briefly in the following sections.

Informal Processes

HHS repeated its intention that the Office of Civil Rights (OCR) and the Centers for Medicare & Medicaid Services (CMS) resolve any compliance issues through informal means, including, for example, “demonstrated compliance, or a completed corrective action plan or other agreement.” The Enforcement Rule makes clear, however, that entering into a compliance plan would not resolve the issue of noncompliance – the action plan or agreement would need to be fully performed. Moreover, in interpreting the strong language of the statute, HHS states that HIPAA “require[s] the Secretary to impose a civil money penalty on any covered entity which the Secretary determines has violated an administrative simplification provision, unless the covered entity establishes an affirmative defense.” There are only two means of avoiding this result: *Completing* a plan of correction and/or reaching a settlement with the Secretary.

The Enforcement Rule also notes that while current compliance and enforcement activities are largely complaint-based, HHS “may also . . . conduct [] compliance reviews to determine if a covered entity is in compliance.” It provides no additional information regarding such compliance reviews, or the basis on which they would be initiated. The AHA believes HHS should give hospitals additional information on how these reviews will be conducted and how entities will be selected for such reviews.

HHS promises to “continue to work on educational and technical assistance materials, including additional guidance on compliance and enforcement and targeted technical assistance materials focused on particular segments of the health care industry.” The AHA is pleased that, as it has repeatedly encouraged, HHS intends to provide additional guidance and assistance. But the

association is disappointed that OCR and CMS have, thus far, failed to provide assistance in several key problematic areas that the AHA identified.

Publicity of Penalties Imposed

In comments about the interim enforcement regulations published in 2003, the AHA asked that HHS make available to hospitals and other covered entities information about the findings of violations, proposed solutions, and good practices in a form that does not identify the violator. Instead, however, the Enforcement Rule will make fully available to the general public information about the imposition of a CMP, including the identity of the hospital or other covered entity and the reasons for the penalty. HHS suggests that this information will be useful “to anyone who must make decisions with respect to covered entities.” Specifically, HHS states that “knowledge of the imposition of a civil money penalty for violation of the Privacy Rule could be important to health care consumers, as well as to covered entities throughout the industry.”

This approach, however, fails to recognize that most Privacy Rule violations that are subject to CMPs likely will be technical in nature, and not result in impermissible use or disclosure of a patient’s protected health information. The methodologies used to establish violations and penalties, including statistical sampling and the number of days a requirement was not met, are not simple to understand. As a result, a published violation could assert that during a three month period Hospital ABC had 1,110 violations of the Privacy Rule – which may mean nothing more than that the hospital failed to document properly that the Notice of Privacy Practices was acknowledged by those admitted to its emergency department. It could also mean that HHS has determined that the hospital’s data collection processes for the accounting of disclosures with respect to 1,110 patients do not have all of the details needed to comply with HHS guidance. As a result, the statement that “Hospital ABC paid several thousand dollars due to 1,110 violations of the Privacy Rule” arguably is misleading and calculated to panic individuals into distrusting their provider.

The AHA appreciates that compliance with all requirements of the administrative simplification provisions, including the technical requirements of the Privacy Rule, is important, and that accrediting entities need to know these facts. The potential for seriously misleading the public with respect to the meaning of Privacy Rule violations where no impermissible use or disclosure occurred, however, is an unwarranted and irresponsible policy. The AHA encourages hospitals to submit comments urging CMS to take a more temperate approach in this matter.

Liability for Others

Business Associates. The AHA is pleased that HHS responded to its previous comments by clarifying in the Enforcement Rule that hospitals and other covered entities are not liable for the actions of their business associates, including clearinghouses, so long as the hospitals take certain actions required by the Privacy Rule. Specifically, the Privacy Rule requires hospitals that know of a violation by their business associate to attempt to end or cure the violation and, if unsuccessful, terminate the contract or report the problem to the Secretary if termination is not feasible. Thus, if a hospital takes this required action toward its business associates’ violations, the hospital will not be liable for such violations.

Agents. The Enforcement Rule states that covered entities, including hospitals, can be held liable for “the actions of any agent, including an employee or other workforce member, acting within the scope of the agency or employment.” This would include independent contractors and volunteers working on-site that a hospital has designated as part of its workforce. HHS proposes using the

Federal Common Law of Agency to impose liability on hospitals for the actions of their agents and employees, rather than relying on varying state laws that otherwise would apply to the relationship between the hospital and its employees and/or volunteers. Thus, it is possible that a hospital's applicable state law would not impose liability on the hospital, but that the federal common law would – exposing the hospital to increased unanticipated liability. Depending on how state laws compare to federal laws regarding agency liability, hospitals may want to comment on the use of this federal body of law as a guide for the imposition of liability.

HHS also “specifically request[s] comment on whether there are categories of workforce members whom it would be inappropriate to treat as agents.” The AHA suggests that hospitals comment to HHS on the inclusion of volunteers and independent contractors as agents for imposing penalties. Although hospitals technically may have some control over such individuals when working on-site at the hospital, the hospital's control is not akin to that of an employee or agent of the hospital and, thus, the hospital should not face liability for violations by volunteers and independent contractors so long as the hospital has provided the requisite instruction as required under the Privacy Rule.

Affiliated Single Covered Entities. Under the Enforcement Rule, hospitals that participate in an affiliated single covered entity (ASCE) with other hospitals under common ownership or control will be held jointly and severally liable for violations by the ASCE. In the preamble to the Enforcement Rule, HHS explains that “no covered entity in an affiliated covered entity could avoid a civil money penalty by demonstrating that it was not responsible for the act or omission constituting the violation or that another covered entity member of the affiliated covered entity was the culpable entity.” This, together with the liability of a hospital for agents (including volunteers), could impose significant potential CMP liability on a hospital in a situation where the hospital has no ability to control or influence the actions taken by another facility included in the ASCE.

Moreover, if imposition of penalties is made public as proposed (see previous discussion), the hospital could be identified as receiving a penalty for violations of the Privacy Rule, but the penalty would actually be for a violation by another facility. The AHA is concerned about the potential liability exposure hospitals would face under this proposal and the potential effect on hospital business if the public is not aware that one hospital received a penalty for another facility's violation. The ASCE structure is one of the “fictions” created by the agency to make it feasible to implement the complex requirements of the Privacy Rule in modern medical environments. It is unwarranted to substitute this regulatory fiction for the corporate form and structure, which establish the basis for enterprise liability under the laws of the United States.

Organized Health Care Arrangements. Participating in an organized health care arrangement (OHCA) does not make the hospital liable for the violations of other members of the OHCA. However, the Enforcement Rule states “it may be a factor considered in the analysis.” It is unclear what HHS intends by this statement, and the AHA is concerned that HHS may use the fact that a hospital is participating in an OHCA with another person or entity that violates HIPAA in order to impose liability on the hospital. For example, suppose a physician agrees to a patient's request for restrictions on use of a patient's information by the hospital, but fails to take the necessary steps under the hospital's HIPAA procedures for ensuring that the request is implemented. The Enforcement Rule makes the hospital's interests adverse to those of the physician; the hospital will have to aggressively defend itself from the imposition of penalties in order to avoid an unjust result. Most hospitals participate in an OHCA with other entities or individuals (e.g., physicians with privileges at the hospital) and, historically, often have faced significant challenges in ensuring that medical staff comply with the hospital's procedures. Clarification of this statement is essential to ensure that participation in an OHCA does not increase hospitals' potential exposure to liability. The AHA urges hospitals to request HHS clarification of this statement.

Procedural Matters

The AHA is concerned about a number of specific requirements, and will carefully evaluate them. Examples include: (1) HHS' statement that "testimony and other evidence obtained in an investigational inquiry may be used by HHS in any of its activities and may be used or offered into evidence in any administrative or judicial proceeding;" (2) HHS's discretion to define "identical requirement" and to count number of violations for purposes of the statutory cap and CMPs; and (3) Limitations on the authority of an administrative law judge in imposing CMPs.