# PROMISES UNDER PRESSURE

## *Ensuring Privacy, Security and Administrative Simplification*

AHA
Advancing Health in America

## HIPAA

**Issue**

For America's hospitals, 2003 is the year of implementation for the Health Insurance Portability and Accountability Act (HIPAA). On April 14, all hospitals were required to be compliant with the medical privacy rules. On April 16, hospitals[1] were required to begin testing their standardized transactions. By October 16, all hospitals must be fully compliant with the electronic transactions and code sets standards. Compliance with these standards includes implementation of all modifications and technical corrections that were published by the Department of Health and Human Services (HHS) on February 20.

With the February publication of the final HIPAA security regulation, hospitals have now accelerated their efforts to address the security of their information systems. Hospitals waited for more than two years for the final rule's release, and they have until April 20, 2005 to comply with it.

**AHA View**

Hospitals' HIPAA implementation and compliance efforts have been hindered by significant problems and delays in the rulemaking process. For example, despite acknowledging that the medical privacy rule was seriously flawed and committing publicly to fixing it, HHS did not publish final changes to the rule until mid-August 2002. HHS then took until December 2002 to issue guidance to address questions and concerns regarding implementation. The guidance provided few new clarifications and generally reiterated much of the information already set forth in the preamble to the August 2002 final rule. Hospitals, although welcoming most of the final rule changes, have not been afforded the full two years to make steady progress towards full compliance that Congress intended when enacting HIPAA.

In addition, hospitals have had to move ahead to meet their medical privacy obligations in the absence of any final rules on security. Because the security rules are inextricably linked to the medical privacy rules, the failure to expedite the release of the final security rules further confounded hospitals' efforts to meet their HIPAA privacy obligations.

Equally important, many hospitals report that information systems and software vendors were reluctant to modify their products to conform to the revised technical specifications included in the addenda to the transactions implementation guides until the modifications and corrections to the electronic transactions standards were made final by HHS. Delays in publishing these changes until late February 2003 raised hospitals' anxieties about whether vendors can complete necessary product modifications within the brief time remaining for compliance. In addition, hospitals are increasingly concerned about having sufficient time for proper testing of their electronic billing systems to ensure that any transactions they submit to payers are not rejected as non-compliant, potentially leaving hospitals with mounting unpaid claims after the October 2003 compliance date.

**AHA View**
*(con't)*

**STATUS OF HIPAA REGULATIONS**

| Standard | Proposed Rule Publication Date | Final Rule Publication Date | Compliance Date |
|---|---|---|---|
| Privacy | November 3, 1999 | August 14, 2002 | April 14, 2003 |
| Transactions and Code Sets | May 7, 1998 | February 20, 2003 | October 16, 2003 (extended deadline) |
| Security | June 16, 1998 | February 20, 2003 | April 20, 2005 |
| National Employer Identifier | August 12, 1998 | May 31, 2002 | July 30, 2004 |
| National Provider Identifier | May 7, 1998 | Unknown | Two years after final rule |
| Claims Attachments | Expected Summer 2003 | Unknown | Two years after final rule |
| National Health Plan Identifier | Expected Summer 2003 | Unknown | Two years after final rule |

**Electronic Transactions Standards**

Hospitals' greatest concern about implementing standardized transactions is the possible disruption to current claim submission and payment cycles that might result from poor, improper or incomplete implementation of the standardized code sets and electronic formats by parties involved in claims adjudication. For hospitals, maintaining proper cash flow is critical to ensure that patient care and essential operations are not compromised. Even slight decreases in claims processing volumes or lengthening of payment cycles hinder hospitals' ability to care for their patients. HHS needs to focus immediately on developing a comprehensive contingency plan that clearly outlines remedial actions that every health plan must take to ensure that an adequate payment level to hospitals is maintained as the field transitions to HIPAA-standardized claims. In addition, the AHA believes that health plans need to identify specifically any deficiencies in rejected transactions so that providers may make necessary corrections and resubmit compliant claims in a timely manner.

Hospitals' longstanding support for standardized transactions, claims attachments and national identifiers was premised on the belief that standardization would eventually lead to significant efficiencies and savings to hospitals. The electronic transactions standards are the only part of HIPAA expected to result in long-term cost savings for providers. The full savings and efficiencies may not be fully realized, however, unless HHS outlines clear "business rules" that establish responsibilities and expectations for payers, providers and others using standardized transactions.

**AHA View** *(con't)*

*Claims Attachments.* The AHA urges HHS to expedite the release of the claims attachments regulation. Hospitals need to know in advance what data they are to collect and report, and the standard should include clear definitions of the events or situations triggering the need for additional reporting. Payers' requests for claims attachments should be limited to rare and unusual circumstances, and there should be a clear business purpose for the information requested. Payers should not be permitted to request additional information in an attachment if that data is already included on the claim or can be derived from information contained on the claim. Without a clear articulation of these limitations, the claims attachments standard will likely be another means to delay processing and payment of claims.

*Prompt Payment.* Hospitals' experience with late payment, incomplete payment, lost claims, etc., also indicates the need for HHS to link standardization directly to the prompt payment of claims. Rules related to prompt payment should:

- Require health plans to accept a HIPAA-compliant claim as a "clean claim" for purposes of contractual provisions with other covered entities under HIPAA, and for state and federal prompt pay requirements;
- Establish a reasonable timeframe for processing and paying the claim; and
- Allow covered entities to file grievances about inappropriate actions with an oversight body that has local review capability.

**Medical Privacy Regulations**

The AHA appreciates the sensitivity and responsiveness HHS has shown to concerns raised by hospitals about the privacy rule's harmful effects on patient care and essential hospital operations. The AHA continues to bring to HHS' attention serious unintended consequences of the privacy rule.

The AHA has asked HHS to modify requirements related to accounting for disclosures of protected health information. Hospitals are required by law to report to public health authorities information for dozens of widely accepted health-related purposes, such as tracking births, deaths, cancer patterns, child abuse and defects in medical devices. The privacy rule would require hospitals to create a burdensome paperwork system to account for such disclosures. The accounting of disclosures requirement could also, according to state public health officials, discourage participation in important public health projects such as reporting initiatives to detect potential bioterrorism-related outbreaks and to measure and improve patient safety.

The AHA supports enabling patients to learn more about the information hospitals must report to public health authorities. HHS' current requirement for accounting for disclosures is not the best way to accomplish this. We are urging HHS to adopt a more practical and less burdensome method to provide patients with meaningful information about what data hospitals must share with public health authorities.

**AHA View**
*(con't)*

In addition, the AHA continues to urge HHS to develop a plan to resolve quickly other unintended consequences that may emerge post-compliance, such as the potential impact that the rule may have on hospitals' ability to raise funds. Philanthropic funds sustain patient care initiatives and support service innovations and new expansions. Given already inadequate and continually eroding reimbursement levels, sustainable fundraising initiatives are essential for all hospitals' viability.

The AHA is also recommending that HHS adopt a flexible approach to enforcement of the medical privacy rule during the two years following the April 2003 compliance date. This additional time could be used for educational activities, including helping patients better understand how the new rule will affect their care. In light of HHS' substantial delays in fixing the rule, it is imperative that HHS explicitly and publicly commit to a flexible enforcement approach that extends over the next two years.

***Security***

The AHA is pleased that the final security rule simplifies or eliminates several administrative requirements that were duplicative or confusing in light of the privacy rule, and that the privacy and security rules are now more compatible. However, we are disappointed that the long delay – more than two years – in issuing the final security rule unnecessarily strains hospitals' already scarce resources.

Failure to expedite the release of the final security rule means hospitals face needless added costs to modify the "reasonable safeguards" required by the privacy rule to comply with the security rule. The final security rule requires hospitals to perform a number of tasks that clearly mirror and even duplicate tasks already performed as part of their efforts to comply with the privacy rule. For hospitals, these tasks certainly could have been performed more efficiently as part of a comprehensive compliance effort focused simultaneously on both privacy and security concerns. The additional implementation burdens caused by the delayed release of the final security rule make an even stronger argument for a flexible approach to enforcement of the privacy rule.

[1] Applicable to providers that in October 2002 requested an extension for complying with the electronic transactions standards.