

First HIPAA Compliance Deadline Is October 16; Extension Requests Due October 15

2002-10-04

The health care industry has been bracing for new regulations since Congress passed the [Health Insurance Portability and Accountability Act](#) (HIPAA) in 1996. The law contained “Administrative Simplification” provisions intended to streamline and automate health care transactions and required the Department of Health and Human Services (HHS) to issue regulations to standardize electronic health care transactions, protect patient privacy, and ensure data security. The compliance date for the first of these regulations is October 16, 2002.

As the various HIPAA compliance deadlines approach, health plan administrators in all industries are discovering HIPAA’s broad reach. Companies and their health plans must act now:

- to determine whether they are covered by HIPAA;
- to consider obtaining an optional one-year extension for some of HIPAA’s requirements; and
- to prepare to comply with HIPAA’s privacy rules and other requirements.

HIPAA applies to

- health care providers (such as hospitals and physicians) that conduct health transactions electronically,
- health plans, and
- health care “clearinghouses” that convert health care data between HIPAA-compliant and non-compliant formats.

Collectively, these are HIPAA’s “Covered Entities.” Although HIPAA does not apply to employers as such, most insured and self-insured employer-sponsored group health plans (including dental plans, health flexible spending arrangements, and other plans providing health benefits) are subject to HIPAA. Only self-administered plans with fewer than 50 participants are exempt. “Small” health plans have an extra year to comply; a small health plan is one that has [no more than \\$5 million in annual receipts](#). Employer-sponsored group health plans with 500 or fewer participants are likely to be “small” under this standard.

Transaction and Code Set Regulations

In August 2000, HHS issued [final rules](#) to harmonize the electronic data interchange (EDI) systems used to conduct certain key health care transactions. These “transaction and code set” regulations will require Covered Entities to use designated data standards and coding systems for conveying health care information in connection with the following types of transactions: (1) health care claims or equivalent encounter information, (2) health care payment and remittance advice, (3) coordination of benefits, (4) health care claim status, (5) enrollment and disenrollment in a health plan, (6) eligibility for a health plan, (7) health plan premium payments, (8) referral certification and authorization, (9) first report of injury, and (10) health claims attachments.

As originally issued, the transaction and code set rules required most Covered Entities to comply by October 16, 2002. The compliance date for small health plans is October 16, 2003. In late 2001, Congress passed the [Administrative Simplification Compliance Act](#), which authorized HHS to extend the transaction and code set compliance date to October 16, 2003 for all Covered Entities.

To obtain this extension, Covered Entities (other than small health plans already subject to the October 16, 2003 deadline) must submit a “compliance plan” to HHS on or before October 15, 2002. The Centers for Medicare and Medicaid Services, the HHS agency that runs the Medicare and Medicaid programs, has developed an online model compliance plan that may be used for this purpose. Extensions will be granted to all submitters of compliance plans, but submitters must agree to begin to test their systems for compliance no later than April 16, 2003. Covered Entities are responsible for retaining service providers that can comply with the new rules. Many third party administrators, insurers, providers, and vendors may be able to assure health plans and other Covered Entities that they can already comply with the HIPAA requirements.

Privacy Standards

In December 2000, HHS issued a comprehensive [regulation](#) intended to protect the privacy of individually-identifiable health information. These regulations were addressed in our [November 2, 1999](#) and [May 31, 2001](#) Internet Alerts. The privacy rules will require Covered Entities to:

- inform individuals how individually-identifiable information about them is used and disclosed;
- limit the use and disclosure of individually-identifiable health information;
- implement internal privacy policies and procedures;
- ensure individuals’ rights to access and amend their information; and
- obtain written authorizations for a wide range of uses and disclosures.

These rules will be enforced by the HHS Office of Civil Rights. Violations may lead to civil or criminal penalties.

Although only Covered Entities are directly subject to the HIPAA privacy rules, HIPAA privacy safeguards will proliferate through contractual provisions that Covered Entities are required to include in their agreements with third party “business associates” that need access to individually-identifiable health information in order to provide services to Covered Entities. Covered Entities have already begun to secure written “business associate agreements” with their contractors and service

providers, and some Covered Entities are tightening their data disclosure policies as their privacy compliance initiatives proceed.

In an attempt to address several controversial provisions of the privacy regulations, HHS issued a significant revision in August 2002. Despite these recent changes, HHS did not extend the compliance deadline for the privacy rules. Accordingly, Covered Entities must comply with the privacy standards by April 14, 2003, except for small health plans, which must comply by April 14, 2004. The one-year extension described above has no effect on the compliance dates for the HIPAA privacy standards. There is presently no mechanism for extending the privacy compliance deadlines.

Data Security Standards

HHS proposed [health data security standards](#) in August 1998, but these rules have not yet been finalized. The compliance date will be two years after the final rules go into effect (three years for small health plans). These regulations will prescribe administrative procedures, physical safeguards, technical security services, and technical mechanisms to preserve the integrity and availability of health data and to protect against breaches of confidentiality and privacy. As proposed, these regulations will also prescribe digital signature standards for Covered Entities that elect to use digital signatures. Digital signatures and other electronic contracting mechanisms were addressed in our [May 28, 2002 Internet Alert](#).

HIPAA's "Administrative Simplification" requirements are complex, far-reaching and even controversial. The October 15 deadline for extending the transaction and code set compliance date is only the first of several approaching HIPAA milestones. Six years after the law was passed, whether companies are ready or not, HIPAA has arrived!

Authors



Barry J. Hurewitz

PARTNER

✉ barry.hurewitz@wilmerhale.com

☎ +1 202 663 6089



Amy A. Null

PARTNER

✉ amy.null@wilmerhale.com

☎ +1 617 526 6541

Linda K. Sherman

RETIRED PARTNER

☎ +1 617 526 6000