WILMERHALE

Health Care Industry Gears Up for a Series of HIPAA Deadlines

2003-03-31

Companies that handle individually identifiable health records have only two more weeks to finalize their policies and procedures for complying with new Department of Health and Human Services (HHS) regulations under the "Administrative Simplification" title of the Health Insurance Portability and Accountability Act, or "HIPAA." As HIPAA regulatory deadlines begin to arrive, companies involved in the health care industry are experiencing one of the most sweeping new health care regulations since Medicare was created in the 1960s.

As discussed in our October 4, 2002 Internet Alert, the HIPAA regulations apply to "covered entities," which include health care providers that conduct certain transactions electronically, health care clearinghouses that convert data between HIPAA-compliant and non-compliant formats, and health plans.

Privacy Rule Compliance Deadline is April 14, 2003

Most covered entities must comply with the HIPAA Privacy Rule by April 14, 2003. (The compliance date is April 14, 2004, for small health plans with $5 million or less in annual receipts). Uses and disclosures of HIPAA-protected health information will be restricted as of that date, and covered entities must have written privacy policies and internal data-handling procedures in place.

Covered Entities Seek Assurances from Business Associates

The impact of the HIPAA Privacy Rule extends far beyond covered entities, because the regulations require covered entities to obtain specific contractual assurances that third party "business associates" will safeguard any protected health information they handle. Among these assurances, business associates must be required to:

- limit uses and disclosures of protected health information to specific authorized purposes;
- implement "appropriate safeguards" to protect information against unauthorized access;
- report unauthorized uses or disclosures of protected health information;
- support the covered entity's obligations to facilitate patients' rights to access, amend, and obtain an accounting of disclosures of protected health information;
- make records available to HHS in connection with HIPAA enforcement activities;
- return or destroy protected health information at the conclusion of the relevant agreement; and
- impose the same limitations on subcontractors and agents that receive protected health information.

Covered entities are now rushing to execute business associate agreements, frequently containing language suggested by HHS.

Beware: Business Associate Agreements May Not be Required

Some covered entities may seek business associate agreements from virtually all of their vendors, suppliers, and service providers, but the HIPAA Privacy Rule does not always require the agreements. Even when business associate agreements are required, they might not be required by the April 14 deadline. HHS guidance confirms that not all relationships with covered entities are business associate relationships. A third party is a business associate of a covered entity only if it:

- uses or creates protected health information for or on behalf of a covered entity, and
- performs certain functions or activities of a covered entity or performs certain services for a covered entity. Business associate functions include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing. Business associate services are legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial services.

Business associate agreements are not required when protected health information is disclosed to a health care provider for treatment of an individual.

For written contracts in force prior to October 15, 2002, business associate assurances, if required, may be added when the contract is next renewed or modified, as late as April 14, 2004.

Moreover, covered entities may seek business associate assurances that extend beyond the mandate of the HIPAA Privacy Rule. For example, covered entities frequently request business associates to indemnify them for all privacy-related violations. In fact, covered entities are not liable under the HIPAA Privacy Rule for the actions of their business associates. To the extent that a business associate agreement is not required or contains provisions not specifically required by the HIPAA Privacy Rule, the terms are negotiable.

Transaction Testing Deadline Also Looms

Just two days after the HIPAA Privacy Rule compliance date, covered entities will face an important deadline for implementing the standardized code sets and transaction formats required under the HIPAA Transaction and Code Set Rule. Covered entities that elected the one-year extension authorized under the Administrative Simplification Compliance Act must begin their internal testing programs no later than April 16, 2003. All covered entities must use the standard code sets and transaction formats by October 16, 2003.

Final Security Rule Begins Another Countdown

Finally, the long-awaited HIPAA Security Rule was issued on February 20, 2003. Covered entities must comply with new data security standards by April 20, 2005, except for small health plans, which must comply by April 20, 2006. The HIPAA Security Rule complements the HIPAA Privacy Rule by setting administrative, physical, and technical standards for protecting health information from unauthorized access, use, disclosure, alteration, or

destruction. Unlike the August 1998 proposed rule, the HIPAA Security Rule distinguishes between "required," or mandatory, standards and "addressable" standards that can be flexibly implemented to meet the particular characteristics and needs of a covered entity. Notably, standards for encrypting health data are addressable, and standards for implementing electronic signatures were postponed for future action.

April 2003 begins a new era of comprehensive U.S. federal regulation of personal data in commerce. Like the consumer financial sector, which already operates under pervasive federal and state privacy regulations (see our June 28, 2001 Internet Alert), the health care industry will now use and disclose information under a federal regulatory regime. The patchwork of U.S. information regulation grows ever more intricate.

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089