WILMERHALE

Federal Economic Stimulus Legislation Broadens HIPAA Health Data Privacy and Security Regulations While Boosting Health IT

2009-02-24

The American Recovery and Reinvestment Act of 2009, the federal economic stimulus legislation that President Obama signed on February 17, 2009, provides over $22 billion to develop, implement, and promote a new health information technology infrastructure, including nationwide electronic health records, by 2014. To address the privacy and data security challenges presented by an electronic health record system, the new law also mandates significant changes in the health data privacy and security regulations issued under the Health Insurance Portability and Accountability Act (HIPAA), and extends those regulations directly to contractors and service providers that handle health data.

The legislation reinvigorates the Office of the National Coordinator for Health Information Technology (ONCHIT) in the Department of Health and Human Services (HHS) as the center of the national health information technology effort. ONCHIT will adopt national standards for electronic health records. The first such standards must be issued by December 31, 2009.

Existing HIPAA regulations already impose national standards for conducting electronic health care claims and other transactions, protecting the privacy of individually identifiable health information, and safeguarding the security of health information maintained or transmitted electronically. The HIPAA regulations, however, apply directly only to "covered entities," which include health plans, health care providers that conduct electronic transactions, and health care clearinghouses that format health data in accordance with electronic transaction standards. Employers, personal health record vendors, and an array of subcontractors and service providers have not been directly subject to federal health data regulations.

The new legislation significantly expands the reach of federal health data regulation and directly regulates business associates for the first time:

Direct Regulation of Business Associates: HIPAA-covered entities engage a wide range of contractors and service providers to generate or handle individually identifiable health information. Previously, these "business associates" were subject only to contractual commitments to act in accordance with certain HIPAA privacy and security standards. The new law retains the requirement for business associate agreements, but makes business associates directly subject to federal regulatory enforcement. Specifically, business associates will be required to adopt HIPAA-compliant administrative, physical, and technical security measures for electronic health data in the same manner as the covered entities for which they work. HHS will issue annual guidance on the most effective and appropriate technical data security measures, such as techniques for encrypting identifiable health data. The new law also makes business associates directly accountable to federal regulators for certain privacy-related violations.

Mandatory Data Security Breach Notification: In keeping with the proliferation of state laws requiring the disclosure of breaches of personal data security, the law obligates covered entities to notify affected individuals and HHS whenever their "unsecured" health information is exposed through unauthorized access, acquisition, use, or disclosure subject to exceptions for certain inadvertent disclosures to the covered entity's employees or within the same facility. These mandatory notification requirements do not apply to security incidents involving "secured" health information that is protected by technologies, such as encryption, that render the contents unusable, unreadable or undecipherable to unauthorized individuals. HHS is required to issue guidelines defining the permissible types of encryption and other technical security measures. Any required notification to individuals must be delivered "without unreasonable delay," which may vary from case to case, but may not exceed 60 days after discovery of the breach. In addition, covered entities must notify prominent media if a breach involves more than 500 residents of a particular state or jurisdiction. Business associates may notify affected covered entities, rather than attempting to contact individuals directly. These new notification requirements should provide added incentives for covered entities and business associates to adopt protocols for encrypting health data.

Breach Notification Obligations Applicable to Personal Health Record Providers: The new law recognizes the emergence of new consumer-facing personal health record (PHR) technologies and imposes obligations on PHR vendors that might be neither covered entities nor business associates. Under the law, PHR vendors must notify affected consumers when they discover a breach of unsecured PHR data. The Federal Trade Commission (FTC), rather than HHS, will serve as the primary federal regulator for PHR vendors that are not covered by the HIPAA regulations. The FTC is required to develop formal PHR breach notification regulations within 180 days.

Notably, the notification requirements applicable to PHR vendors will be in addition to the FTC's "Red Flags" regulations, which apply broadly to financial institutions and creditors, including any entities that collect payments for services after the services are rendered. The Red Flag rules require entities, including health-related entities, to adopt programs for identifying and addressing security risks that might lead to identity theft.

Expanded Right to Accounting of Disclosures: HIPAA regulations currently permit individuals to request an "accounting" of disclosures of their health information, excluding certain disclosures such as those made in connection with treatment, payment or certain administrative health care operations. The new law permits an individual to obtain an accounting of disclosures of electronic

health records, even if such disclosures were made for treatment, payment or health care operations.

New Limits on Marketing and Selling Health Data: The existing HIPAA regulations generally require prior written authorization before covered entities may sell or otherwise disclose protected health information for marketing purposes, but creates a broad exception for a wide range of communications about products or services offered by the covered entity making the communication. These excepted communications are currently treated as health care operations for which no individual authorization is required. The new law further limits the types of communications that can be treated as health care operations, but allows covered entities to continue to receive payments from third parties, such as pharmaceutical companies, for communicating with patients about drugs or biologics for which the targeted individual has a current prescription. The law generally requires an individual's prior written authorization before either covered entities or their business associates may disclose protected health information in exchange for compensation, but this authorization will not be required for compensated disclosures made for certain purposes including public health, research, treatment, and certain administrative operations, provided that payments made for research data are limited to reflect the costs of preparation and transmittal of the data. HHS is required to study whether payments for public health-related disclosures should be limited in the same manner.

Expanded Enforcement: The new law provides for enhanced enforcement of health information privacy and security regulations, with newly defined tiers for imposing civil penalties and new authority for state attorneys general to pursue injunctive and monetary claims to combat privacy and security violations involving health data.

The massive economic stimulus legislation provides funding for an unprecedented commitment to implementing electronic health records on a national level while launching the most sweeping changes in health data privacy and security law since the HIPAA regulations were authorized in 1996. Any entity that handles health information should prepare for several months of intense regulatory activity as the new law is implemented and HHS and FTC regulations are developed.

Authors

Barry J. Hurewitz

PARTNER

barry.hurewitz@wilmerhale.com

+1 202 663 6089