

Health Law Washington Beat: Recent Health Industry News

2/26/2009

In This Issue

- President Obama Signs the American Recovery and Reinvestment Act of 2009—Act Includes Billions of Dollars in Funding for the Promotion of Health Information Technology
- Act Expands HIPAA Privacy and Security Rules
- Act Includes Incentives for Medicare and Medicaid for Certified Use of Electronic Health Records

President Obama Signs the American Recovery and Reinvestment Act of 2009—Act Includes Billions of Dollars in Funding for the Promotion of Health Information Technology

The American Recovery and Reinvestment Act of 2009¹ (the “Act”) that was signed into law on February 17, 2009 by President Obama provides for \$787 billion in spending and tax incentives to help boost the economy. One of the most anticipated provisions of the Act relates to the national implementation of health information technology (HIT). The Act provides \$2 billion in start-up funds to the Department of Health and Human Services’ (HHS) Office of the National Coordinator of Health Information Technology (ONCHIT) to promote and implement HIT,² with a goal of utilization of an electronic health record by each person in the United States by 2014. In addition, the Act specifically calls upon the National Coordinator (head of ONCHIT) to implement the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

HIT Extension Program and Regional Extension Centers

The HITECH Act provides organizations several opportunities to obtain federal grants or contracts to promote and implement HIT. For instance, HHS and ONCHIT will collaboratively establish a HIT extension program to provide HIT assistance to healthcare providers. The program will include assistance from entities such as a HIT Regional Extension Center (Center), which would provide technical assistance and best practices to support and accelerate efforts to adopt, implement, and effectively utilize HIT by providers. In order to be considered a Center, an organization must be affiliated with a U.S.-based non-profit institution that is awarded an implementation grant (discussed in more detail below) under the HITECH Act. In addition, before it can become a Center, an organization also must satisfy the criteria that HHS must publish in the Federal Register within 90 days of enactment of the HITECH Act.

Centers could receive from HHS a maximum of 50% of the capital and annual operating and maintenance costs for creating and maintaining the Center for up to four years.

State Planning and Implementation Grants to Promote HIT

The HITECH Act allows HHS to also award planning or implementation grants to a state or qualified state-designated entity to assist in the expansion of the electronic exchange and use of health information. Such assistance includes:

- enhancing broad participation in the national electronic use and exchange of health information;
- providing technical assistance in the development of solutions to exchange electronic health information;
- assisting patients in using HIT; and
- promoting the use of electronic health records for quality improvement measures.

HIT Policy and Standards Committees

In addition to the funding provisions, the HITECH Act also outlines the expectations and duties of the National Coordinator to promote HIT and establishes both a HIT Policy Committee and a HIT Standards Committee. Each committee will make recommendations to the National Coordinator related to: (a) the implementation of a national HIT infrastructure, including how to reach the goal of each person using electronic health records by 2014; and (b) standards, specification, and certification criteria for the electronic exchange of health information.

Medicare and Medicaid Provider Payments

The Act also provides payments to Medicare and Medicaid providers who demonstrate use of certified electronic health records. See Mintz Levin’s Client Advisory, Stimulus Bill Passed by Congress Includes Medicare and Medicaid Incentives for Certified Use of Electronic Health Records.

Other Appropriations for HIT

In addition to the funds appropriated to HHS, the Act provides funding to other agencies to promote HIT. The other appropriations include:

- \$4.7 billion to the National Telecommunications and Information Administration for the “Broadband Technology Opportunities Program”;
- \$85 million to the Indian Health Service for health information technology activities such as telehealth services development and related infrastructure requirements;
- \$2.5 billion to the Health Resources and Services Administration for grants to health centers, construction, renovation and equipment, and for the acquisition of health information technology systems, for health centers; and
- \$2.5 billion to the Rural Utilities Service for broadband loans, loan guarantees, and grants for broadband infrastructure in any area of the United States.

Implementation Challenges

The road to implementing these HIT provisions will be a rocky one. The existing hesitation of healthcare providers in adopting HIT, coupled with the withdrawal of Tom Daschle’s nomination as the Secretary of HHS, present many obstacles for a quick and efficient implementation process. However, as the industry begins to realize the benefits of utilizing HIT (e.g., reduction in medical errors, quality improvement, and efficiency) and the existence of added privacy and security protections provided under the Act, the adoption and use of HIT should grow exponentially. The opportunities included in this Act for the HIT industry are infinite and Mintz Levin, as a leading advisor in this space, will continue to track the implementation and development of these and other related provisions.

Act Expands HIPAA Privacy and Security Rules

The Act includes a series of health information privacy provisions aimed at closing perceived gaps in the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996³ (HIPAA). These provisions will have a significant impact not only on health care organizations that are obligated to comply with HIPAA (Covered Entities) but also on third party services providers, or “Business Associates,” who use or disclose health information on a Covered Entity’s behalf. Among other things, the Act imposes elaborate notification obligations in the event of a security breach and extends substantive privacy and security compliance obligations to business associates. Additionally, the Act strengthens HIPAA federal enforcement and grants new enforcement powers to the states. There are certain exceptions for various provisions within the Act, but generally the effective date for these changes is 12 months following enactment of the legislation, which occurred on February 17, 2009.

Breach Notification

Under HIPAA, Covered Entities have no affirmative obligation to notify patients in the event that their protected health information (PHI) is lost or stolen, or if the privacy and security of the PHI is otherwise compromised. Under the Act, Covered Entities will be obligated to notify affected individuals and the “Secretary of the Department of Health and Human Services (the Secretary)” in the event of a breach of “unsecured” PHI. “Unsecured” PHI is defined as PHI that is not protected by “technologies and methodologies that render Protected Health Information unusable, unreadable, or indecipherable to unauthorized individuals,” for example, unencrypted PHI. Notice must be provided “immediately” if a breach involves 500 or more individuals. Otherwise, notice must be provided within 60 days of discovery and must include specific information about the breach and the type of unsecured PHI involved.

New Business Associate Obligations

Generally, HIPAA’s compliance obligations did not apply to Business Associates. The Act applies HIPAA security standards directly to Business Associates, as well as civil and criminal penalties for violations. This will dramatically increase the compliance burden for organizations in the health information technology field and others who provide services to Covered Entities involving the use or disclosure of PHI. The Act also makes Business Associates directly responsible for complying with HIPAA’s implementation specifications for Business Associate Agreements. These specifications include such things as taking steps to end patterns of activity or practices that are in material breach of a Business Associate agreement’s terms, reporting un-curable breaches to the Secretary, or other compliance obligations that were previously the responsibility of the Covered Entity. It is important to note that the Joint Explanatory Statement of the Committee of Conference that was published with the Act states that it was Congress’s intent that the HIPAA Privacy Rule and the Act’s additional privacy requirements apply to Business Associates along with the enforcement provisions. So, the extent of the Privacy Rule’s applicability to Business Associates is an open question that may be further clarified with additional guidance.

HIPAA Enforcement

The Act expanded HIPAA enforcement beyond the federal government and permits a state attorney general to bring a civil action if he or she believes that the interests of one or more state residents is threatened or adversely affected as a result of a HIPAA violation. The state attorney general may pursue injunctive relief or civil damages.

Other new requirements under the Act include the following:

- Mandatory audits by the Secretary of both Covered Entities and Business Associates.

- Mandated HIPAA privacy and security compliance for vendors of “Personal Health Records.” “Personal Health Records” are electronic compilations of health information controlled by patients and not by Covered Entities.

- Expansion of the accounting of disclosures requirement for providers that use or maintain an electronic health record. Such Covered Entities are required to account for disclosures for treatment, payment and health care operations which are presently exceptions to the accounting requirement under HIPAA.

- Prohibition on certain marketing communications when a Covered Entity receives direct or indirect remuneration in exchange for making the communications.

- The right for patients to opt-out of fundraising communications from a Covered Entity.

The enforcement stakes are higher under this new law and to ensure compliance, Covered Entities will need to revisit existing privacy and security policies and forms, such as business associate agreements. Business Associates will face significant new compliance obligations, including the adoption of privacy and security policies and procedures. Mintz Levin is actively seeking clarification on the extent of HIPAA privacy rule applicability to Business Associates and will publish additional information as it becomes available.

Act Includes Incentives for Medicare and Medicaid for Certified Use of Electronic Health Records

Although current legislative initiatives promote the use of health information technology and electronic health records in both the Medicare and Medicaid programs (e.g., e-prescribing standards, pay-for-performance demonstration, and Medicaid Management Information Systems), the Act allows for even more incentives to adopt and implement HIT. For more information on the incentives, see Mintz Levin’s Client Advisory.

Endnotes

¹ P.L. 111-5.

² Health information technology is defined as hardware, software, integrated technologies or related licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by health care entities or patients for the electronic creation, maintenance, access, or exchange of health information.

³ P.L. No. 104-191.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

MEMBERS

Robert D. Clark
Managing Member, Health Law Practice
RDClark@mintz.com

Stephen M. Weiner
Chairman, Health Law Practice
SWeiner@mintz.com

Susan W. Berson
Managing Member,
Washington, D.C. Office
SBerson@mintz.com

Thomas S. Crane
TSCrane@mintz.com

Stephen C. Curley
SCCurley@mintz.com

Deborah A. Daccord
DADaccord@mintz.com

Hope S. Foster
HSFoster@mintz.com

Ellen L. Janos
EJanos@mintz.com

Karen S. Lovitch
KSLovitch@mintz.com

M. Daria Niewenhous
DNiewenhous@mintz.com

Andrew B. Roth
ARoth@mintz.com

OF COUNSEL

Michael D. Bell
MDBell@mintz.com

Margaret D. Kranz
MKranz@mintz.com

ASSOCIATES

Stephen R. Bentfield
SRBentfield@mintz.com

Dianne J. Bourque
DBourque@mintz.com

Shawneequa L. Callier
SLCallier@mintz.com

Theresa C. Carnegie
TCCarnegie@mintz.com

Brian P. Dunphy
BDunphy@mintz.com

Garrett G. Gillespie
GGGillespie@mintz.com

Lauren N. Haley
LNHaley@mintz.com

Rachel M. Irving
RMIrving@mintz.com

Krietta Bowens Jones
KBowensJones@mintz.com

Sarah A. Kaput
SAKaput@mintz.com

Katina W. Lee
KLee@mintz.com

Carrie A. Roll
CARoll@mintz.com

Tara E. Swenson
TESwenson@mintz.com

Andrea P. Testa
ATesta@mintz.com

Melissa O'Neil Thatcher
MOThatcher@mintz.com

Heather L. Westphal
HLWestphal@mintz.com

Jennifer E. Williams
JEWilliams@mintz.com

Nili S. Yolin

NSYolin@mintz.com

© 1994-2009 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C. All Rights Reserved.

This website may constitute attorney advertising. Prior results do not guarantee a similar outcome. Any correspondence with this website does not constitute a client/attorney relationship. Neither the content on this web site nor transmissions between you and Mintz Levin Cohn Ferris Glovsky and Popeo PC through this web site are intended to provide legal or other advice or to create an attorney-client relationship. Images or photography appearing on this website may not be actual attorneys or images associated with Mintz Levin.