



# Health Law Alert

## Legal and political developments affecting the health care industry

A publication of Nixon Peabody LLP

FEBRUARY 2009

### The Health Information Technology for Economic and Clinical Health Act (HITECH Act): implications for the adoption of health information technology, HIPAA, and privacy and security issues

By *Linn F. Freedman*

On February 17, 2009, President Obama signed into law the Health Information Technology and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act. HITECH codifies and funds the Office of the National Coordinator for Health Information Technology (ONC) and provides for the infusion of \$19 billion over a four-year period, in grants and loans, for infrastructure and incentive payments under Medicare and Medicaid for providers who adopt and use health information technology (HIT). It also expands security and privacy provisions and penalties to HIPAA business associates of covered entities. The implications of HITECH for hospitals, health care providers, vendors, health information exchanges (HIEs), and Regional Health Information Organizations (RHIOs) are far-reaching. Provisions of HITECH are summarized below.

Although the ONC was established by Executive Order in 2004, HITECH appropriates \$2 billion to the ONC and codifies the duties of the National Coordinator, with the stated goal of “the utilization of an electronic health record for each person in the United States by 2014.” The ONC strategic plan is to include “the development of a nationwide health information technology infrastructure that allows for the electronic use and exchange of information” that ensures that patients’ health information is secure and protected.

The ONC is responsible for:

- establishing national standards for the exchange of health information;
- coordinating HIT policy and programs, and updating and implementing the Federal Health IT Strategic Plan through collaboration with public and private entities;
- ensuring that privacy and security protections are incorporated in the electronic exchange of health information;
- implementing strategies to enhance the use of HIT;
- assessing the impact of HIT in communities with health disparities;
- evaluating the benefits and costs of the exchange of health information;
- appointing a Chief Privacy Officer of ONC within 12 months;

- establishing an HIT Policy Committee, responsible for making policy recommendations to the ONC on the implementation of a nationwide HIT infrastructure; and
- establishing an HIT Standards Committee, responsible for making recommendations to the ONC regarding standards, implementation specifications and certification criteria for HIT.

Consistent with other existing incentive programs developed by the federal government for the adoption of electronic health records (EHRs), and to implement the ONC's strategic plan for the national adoption of HIT, HITECH also provides for \$19 billion in grants and loan funding for incentives for the use of HIT. The entities that will be eligible for such grants and loan funding include those that support the HIT architecture that will enhance the nationwide electronic exchange of health information, including connecting HIEs; health care providers participating in Medicare, Medicaid, and the State Children's Health Insurance Program (including hospitals and physicians); community health centers; clinical data repositories and registries; and public health departments. The funds provided must meet applicable standards determined by the HIT Standards Committee. Funds distributed will support technology architecture, development and adoption of certified EHRs for providers not otherwise eligible, training, infrastructure, and overall expansion and promotion of technology.

The Health Information Technology Extension Program will also be established to provide assistance and support to accelerate the adoption of HIT through regional centers of technical assistance. These regional centers will be associated with existing or new nonprofit groups and funding provided will be up to 50 percent of the capital, operating, and maintenance funds for up to four years. The criteria for determining qualified applicants will be published within the next 90 days. Beginning on January 1, 2010, the ONC may award grants and loan programs to states for the purchase of certified EHR technology used to exchange health information. Finally, the National Science Foundation is directed to provide assistance in the creation and expansion of medical health informatics education programs at institutions of higher education.

In a substantial change to the current security and privacy regulations under the Health Information Portability and Accountability Act (HIPAA), and in response to increased public awareness and debate over the privacy and security of electronic health information, HITECH requires the application of HIPAA security and privacy provisions and penalties directly to business associates of covered entities. Before HITECH, the security and privacy requirements were imposed on business associates through contractual provisions with covered entities. HITECH requires business associates to restrict the use and disclosure of protected health information (PHI) and subjects business associates directly to civil and criminal penalties for violating HIPAA requirements in the same manner as covered entities. The Secretary of Health and Human Services (HHS) will provide guidance on this requirement within the next year.

Another key requirement imposed by HITECH is for covered entities and business associates to notify individuals and the HHS if an individual's unsecured or unencrypted protected health information "has been, or is reasonably believed...to have been, accessed, acquired, or disclosed as a result of such breach." If the breach affects more than 500 individuals, the notification can be through media outlets. Further, personal health record vendors must notify the individual and the Federal Trade Commission of a breach. Of note is the fact that this provision is far more stringent than the breach notification laws that have been passed by numerous states, which require individual notification if the personal information is reasonably believed to have been used for identity theft

purposes. Most states that have implemented breach notification laws require that the information be used for identity theft purposes before imposing civil or criminal penalties. Compliance with this provision of HITECH may be difficult for covered entities and business associates, although HITECH does not include, in the definition of a breach, an inadvertent disclosure or access to information provided that there is no further access or disclosure.

Other new privacy and security requirements in HITECH include:

- covered entities must honor a patient's request to withhold PHI from a health plan if the patient paid for the medical care;
- covered entities must limit use or disclosure of PHI to a "limited data set" or, if needed, to the minimum necessary to accomplish an intended purpose;
- when requested, covered entities must provide patients with an audit trail of all disclosures of PHI made within the past three years;
- covered entities may not receive payment for communicating with patients for marketing purposes without the specific authorization of the patient (including fundraising solicitations);
- employees of covered entities or other individuals who knowingly access, use, or disclose PHI for improper purposes will be subject to criminal penalties; and
- civil penalties for violations under HIPAA are increased, depending on the conduct. The federal government must impose penalties if the violation of the conduct was willful. State attorneys general (most of whom already have the jurisdiction to prosecute under state privacy laws) are authorized to prosecute and seek civil penalties. The penalties are tiered according to conduct, from \$100 per violation with a maximum of \$25,000 per year, to the maximum penalty of \$50,000 per occurrence and \$1.5 million per year.

HITECH pronounces that organizations that access PHI from covered entities, such as HIEs, RHIOs, e-prescribing gateways, or vendors that contract with covered entities to offer personal health records (PHRs) must have written contracts with the covered entity and will be treated like a business associate. This clears up existing confusion and further promotes the wider adoption of HIT.

In general, the effective date of HITECH is February 17, 2010. However, the incentive payments for practitioners and hospitals will commence in 2011 and phase out through 2015.

HITECH applies to covered entities, including hospitals, health care providers, health plans, business associates, vendors, HIEs, RHIOs, and PHRs. To comply with HITECH, we recommend the following:

- develop and implement a Red Flag Rules Compliance Program;
- develop and implement a Breach Notification Compliance Program;
- review and amend existing business associate agreements and determine if new business associate agreements are needed;
- strategize and position yourself to obtain loan and grant funding through the stimulus; and
- ensure your technology is CCHIT certified.

Further updates, including proposed regulations pertaining to HITECH, will be issued by the government in the near future. We will continue to provide you with updates on HITECH as developments occur. For additional information on this issue or other matters involving health information technology, please contact Linn Foster Freedman at [lfreedman@nixonpeabody.com](mailto:lfreedman@nixonpeabody.com) or 401-454-1108.

\* \* \*

The foregoing summary is provided by Nixon Peabody for educational and informational purposes only. It is not a full analysis of the matter summarized and is not intended, and should not be construed, as legal advice. This publication may be considered advertising under applicable laws.