

# The Metropolitan Corporate Counsel®

www.metrocorpcounsel.com

Volume 17, No. 3

© 2009 The Metropolitan Corporate Counsel, Inc.

March 2009

## Health IT Law Addresses Interoperability, Privacy, Security And Deployment Of Electronic Health Records

Meg Hardon  
and Alysa Z. Hutnik

KELLEY DRYE & WARREN LLP

The Health Information Technology for Economic and Clinical Health Act (HITECH), signed into law by President Barack Obama as part of The American Economic Recovery and Reinvestment Act of 2009, aims to improve healthcare delivery to patients by reducing medical errors, driving down costs, and giving patients greater information about, and control over, their medical records. The new law brings together a wide range of issues and stakeholders in healthcare, information technology, and the government to jump-start widespread adoption of electronic health records (EHR).

Proprietary technology systems, technical standards, and concerns about privacy and data security have long stalled the momentum toward a national electronic health records system. Congress and the Obama administration aim to overcome these barriers by defining standards for a nationwide interoperable and secure system, and building public confi-

*Meg Hardon is a Senior Advisor with the Government Relations & Public Policy practice group at Kelley Drye & Warren LLP and has more than 24 years of experience as a strategic public affairs consultant. Alysa Z. Hutnik is a Senior Associate with the firm's Privacy & Information Security and Advertising Law practices, and serves as chair of the American Bar Association's (Section of Antitrust) Privacy and Information Security Committee.*



Meg Hardon



Alysa Z. Hutnik

dence in the use of EHRs. HITECH, a part of the economic stimulus bill, provides \$19 billion to standardize and secure the creation, access, storage, and sharing of electronic health information.

Many doctors and hospitals across the United States have implemented electronic medical records systems in the past decade but, without national standards on interoperability and use, these records are often unusable by entities outside of the doctor's office or hospital, thereby diminishing the benefits of better care and lower cost.

### Strategy And Milestones

Under the new law, the Department of Health and Human Services' (HHS) Office for the National Coordinator of Health Information Technology (ONCHIT) will now set a charter for health IT policy priorities in the United States. The ONCHIT will be responsible

for reviewing and endorsing health IT standards, updating a health IT strategy and setting milestones, including a goal for the use of EHRs for each U.S. person by 2014, developing a voluntary certification program, and reporting on the progress of HIT implementation. The ONCHIT will fulfill these requirements in cooperation with stakeholders in the U.S. healthcare industry under the auspices of The National eHealth Collaborative (NeHC).

### Funding

HITECH funding includes the development of technical standards to be coordinated by the ONCHIT, and financial incentives to healthcare providers to use EHRs. Doctors, hospitals, and other Medicare and Medicaid providers will receive financial benefits for the use of EHRs starting in 2011, then subsequently be penalized for the failure to use them after 2014.

*Please email the authors at [ehardon@kelleydrye.com](mailto:ehardon@kelleydrye.com) or [ahutnik@kelleydrye.com](mailto:ahutnik@kelleydrye.com) with questions about this article.*

The law also authorizes funding for competitive grants and loans to States to implement the use and exchange of electronic medical data, and supports education and training of healthcare providers through the development and funding of health information technology extension centers across the United States.

### Technology

The technical standards to achieve interoperability and support privacy and security standards for EHRs will be coordinated through the Healthcare Information Technology Standards Panel (HITSP), a public-private entity. While some standards do exist today, the HITSP will examine and harmonize health IT standards for computer infrastructure; data security; computing systems; networking; software; and information management policies that are used to support EHRs.

An initial set of standards, specifications, and certification criteria are required to be adopted by December 31, 2009.

### Privacy And Data Security

Privacy and data security are seen by stakeholders as an integral part of a successful national electronic medical records system. Without public confidence in how their records are used, to whom they are disclosed, and how the records are protected, consumers will not support the use of electronic health records in their own care management. The necessity of securing and defining such controls for electronic medical records, while widely accepted, has been a challenge for policymakers, researchers, healthcare providers, and patients. Indeed, one of the core challenges has centered around how to strike the appropriate balance between protecting the confidentiality, security, and integrity of individual medical information, while also expanding the universe of recipients who would have access to analyze medical data for purposes of health research and related areas. The HITECH legislation makes a bold attempt at striking this balance with a number of robust provisions that add teeth to existing federal healthcare privacy laws, specifically the Health Insurance Portability and Accountability Act (HIPAA).

For example, the Secretary of HHS will be required to issue annual guidance on the most "effective" and "appropriate" technical safeguards that should be implemented to protect individual medical information. While clarity on the nature and type of such safeguards can be help-

ful, such specificity may also serve as a benchmark used by regulators to determine when a business has insufficient security controls, and thus, whether they are in violation of HIPAA. This type of guidance on specific types of technical safeguards goes much further than the information being provided by other relevant federal regulators, such as the Federal Trade Commission (FTC), concerning how personal data should be protected.

In addition, while the majority of states have enacted data breach notification laws, HITECH implements a federal data breach notification standard that is more rigorous in some areas than the state laws. Specifically, a HIPAA "covered entity," its business associate, or a healthcare vendor (*i.e.*, a business, other than the previous two, that offers or maintains a personal health record) will be obligated to notify consumers if medical information in the entity's control is accessed, acquired, or disclosed as a result of a breach (*i.e.*, regardless of whether the information is unlikely to be used for illegal or other nefarious purposes). The entity would need to notify: such consumers within 60 days of discovery of the breach; state media if the breach involves more than 500 residents; and the HHS secretary (and healthcare vendors would need to notify the FTC). Specific details also must be included in the breach notice, including the date of the breach and the date of discovery of the breach.

In addition, business associates will now be directly subject to HIPAA privacy and security requirements (and corresponding civil and criminal penalties for non-compliance), rather than just enforcement under the contract with the HIPAA covered entity.

To address patient concerns about control over their medical data, the law clarifies the circumstances that individuals can restrict disclosure of their personal information by HIPAA covered entities and their agents, and requires HHS to issue regulations on how to account for disclosures of medical information that balance the interests of the individual patients in the circumstances of disclosure versus the administrative burden on businesses in accounting for all such types of disclosure. The law also bans sales of medical information under certain broad conditions unless the entity obtains the individual consumer's express authorization (*i.e.*, a much more rigorous form of clear and unambiguous consent than an opt-out

form of notice).

Finally, HIPAA enforcement gets a sharper edge: the Secretary of HHS will now be *required* to impose penalties for HIPAA violations caused by "willful neglect" and formally investigate any bona fide complaints of "willful neglect," which would include breaches caused by insufficiently protected individual medical information. Moreover, the law allows state attorneys general to enforce violations and seek injunctive relief, damages, and attorneys' fees.

The significant privacy and data security protections achieved in the legislation reflect a growing trend by lawmakers at the state and federal levels to increase protections of personal information. Two recent studies on healthcare information protection specifically reinforce the importance of privacy and data security in the medical sector. The Government Accountability Office issued a Health Information Technology report asserting that privacy protection is essential to the trust that will encourage widespread adoption of electronic medical record use by consumers. Simultaneously but separately, the National Academies of Sciences' Institute of Medicine has called for a new approach for protecting healthcare data with stronger privacy, data security, and accountability standards in all healthcare research. HITECH establishes the framework to build public trust and protect health data.

### Public-Private Collaboration

HITECH is the outcome of a public-private initiative to promote the adoption of health IT systems and, in the process of doing so, improve healthcare. Private healthcare stakeholders will continue to play a significant role in the adoption of such systems, from the establishment of technical standards and development of EHR products, to the deployment of health IT systems. In addition, the policy direction and funding provided in the law may finally remove some of the existing technical barriers and resolve privacy and data security concerns that have limited the adoption of health IT across the United States to date. Overall, the law's significant public investment in these areas is expected to catalyze significant private investment by hospitals and doctors' offices in electronic health records systems, and encourage broad adoption of EHRs by patients across the United States.