



**HEALTHCARE
ATTORNEYS**

Karen S. Rieger
Healthcare Practice
Chair

Kevin D. Gordon
Healthcare Litigation
Practice Chair

Jennifer L. Ivester Berry

Laura Brookins

LeAnne Burnett

Jordan K. Field

Eric S. Fisher

Richard C. Ford

James H. Holloman, Jr.

Alison M. Howard

Christopher B. Keim

Michael S. Laird

Jay W. Larimore

Cori H. Loomis

Jasmine A. Majid

Robert McCampbell

Kenni B. Merritt

Brooke S. Murphy

Cherish K. Ralls

Gary C. Rawlinson

Mary Robertson

Malcolm E. Rosser IV

Timila S. Rother

David A. Shipley

Earl A. Skarky

Roger A. Stong

Rustin Strubhar

HITECH ACT - PART 2

WHAT YOU NEED TO DO TO COMPLY WITH NEW HIPPA REQUIREMENTS

Last month, we issued a client advisory summarizing the provisions of the "Health Information Technology for Economic and Clinical Health Act" or "HITECH Act," which contains significant expansions to the HIPAA privacy and security requirements.

The purpose of this advisory is to inform our clients of actions you need to take in order to be in compliance with the HITECH Act. Although the HITECH Act contains a significant number of requirements, the list below reflects several of the most essential action items that need to be addressed. *The effective date of the action items below is February 17, 2010.*

1. Review and revise your business associate agreements to incorporate the new HITECH requirements.

Pursuant to the HITECH Act, the HIPAA requirements for administrative, physical, and technical information safeguards and written policies and procedures will apply directly to Business Associates, as will the penalties for violations. These requirements need to be incorporated into all business associate agreements.

2. Develop a security breach notification process.

Covered entities and business associates will now have affirmative obligation to notify certain parties of security breaches. A breach requiring notification occurs when there are improper disclosures of unsecured (e.g., non-encrypted) protected health information ("PHI") and/or when there is improper internal acquisition, access or use, such as employees accessing and viewing medical records when they have no need to do so. The new rules require Covered Entities to notify affected individuals within 60 days of a breach and provide notice to the Secretary of HHS. The notification to HHS must take place immediately if it involves more than 500 people. Otherwise, the Covered Entity may maintain a log of breaches involving less than 500 individuals and provide the log to the Secretary of HHS annually. The security breach notice content is specified by the provisions of the HITECH Act.

3. Revise your policy on using PHI for marketing.

The HITECH Act clarifies the circumstances in which a patient's PHI can be used for marketing. These changes will require a revision of many marketing policies.

4. Revise your policy on restriction of disclosures of PHI.

The HITECH Act *requires* covered entities to accept an individual's request for restrictions on disclosures of PHI for payment or healthcare operations *if* the information pertains *only* to a healthcare item or service that the individual has paid for out of pocket in full, *unless* disclosure is otherwise required by law or is for treatment purposes. For example, if a patient has paid for any testing/treatment related to HIV/AIDS, a Covered Entity must comply with the patient's request not to disclose this information to his/her healthcare insurance provider. Policies must be revised to reflect these new restrictions.

5. Revise your policy on the "minimum necessary" standard.

Under the HITECH Act, a Covered Entity must limit its requests for and use or disclosures of PHI to a "Limited Data Set" to the extent practicable. The term "Limited Data Set" currently has no meaning outside of the research context, so the Secretary of HHS is directed in the law to issue guidance, within 18 months, on what constitutes the minimum necessary 'limited data set.'

6. Revise your policy on accounting for disclosures of PHI if you have (or intend to have) an electronic health record ("EHR").

Currently, HIPAA does not require Covered Entities to provide accountings of disclosures for treatment, payment, or healthcare operations. Under the HITECH Act, the exception is eliminated if the Covered Entity maintains an EHR. This will significantly increase the accounting disclosures required of Covered Entities.

7. Ensure that you are not selling PHI.

HITECH prohibits Covered Entities and business associates from selling PHI unless they receive a valid authorization and a statement from the subject of the PHI, stating whether the PHI can be further exchanged or sold by the entity that receives it. The current HIPAA regulations contain penalties for the criminal fraudulent sale of PHI, but do not explicitly prohibit all sales of PHI.

8. Understand the ramped-up enforcement provisions.

To date, enforcement of HIPAA has been complaint driven. Under the heading "Improved Enforcement," the HITECH Act requires the Secretary of the Department of Health and Human Services to periodically audit covered entities and business associates for compliance with HIPAA.

If we can assist you with the implementation of any of the action items listed above, or if you have specific questions regarding the information in this Advisory, please contact Karen Rieger, 405-235-7788, Cori Loomis, 405-234-3832, or any Crowe & Dunlevy attorney who typically handles your legal issues.

This client advisory is published by Crowe & Dunlevy P.C. to inform our clients and friends of important developments in the healthcare industry. The content is informational only and does not constitute legal or professional advice. We encourage you to consult an attorney in the Crowe & Dunlevy healthcare law group if you have specific questions or concerns relating to any of the topics discussed herein.
