Waggoner • Irwin • Scheele
& Associates INC

HHS Issues Rule Requiring Individuals Be Notified of Breaches of Their Health Information

New regulations requiring health care providers, health plans, and other entities covered by the Health Insurance Portability and Accountability Act (HIPAA) to notify individuals when their health information is breached were issued today (August 19, 2009) by the U.S. Department of Health and Human Services (HHS).

These "breach notification" regulations implement provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, passed as part of American Recovery and Reinvestment Act of 2009 (ARRA).

The regulations, developed by the HHS Office for Civil Rights (OCR), require health care providers and other HIPAA covered entities to promptly notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals. Breaches affecting fewer than 500 individuals will be reported to the HHS Secretary on an annual basis. The regulations also require business associates of covered entities to notify the covered entity of breaches at or by the business associate.

"This new federal law ensures that covered entities and business associates are accountable to the Department and to individuals for proper safeguarding of the private information entrusted to their care. These protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information," said Robinsue Frohboese, acting director and principal deputy director of OCR.

The regulations were developed after considering public comment received in response to an April 2009 request for information and after close consultation with the Federal Trade Commission (FTC), which has issued companion breach notification regulations that apply to vendors of personal health records and certain others not covered by HIPAA.

To determine when information is "unsecured" and notification is required by the HHS and FTC rules, HHS is also issuing in the same document as the regulations an update to its guidance specifying encryption and destruction as the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals. Entities subject to the HHS and FTC regulations that secure health information as specified by the guidance through encryption or destruction are relieved from having to notify in the event of a breach of such information. This guidance will be updated annually.

The HHS interim final regulations are effective 30 days after publication in the Federal Register and include a 60-day public comment period. For more information, visit the HHS Office for Civil Rights web site at http://www.hhs.gov/ocr/privacy/

To track the progress of HHS activities related to ARRA, visit www.hhs.gov/recovery. To track all federal activities related to ARRA, visit www.recovery.gov.

Source: http://www.hhs.gov/news/press/2009pres/08/20090819f.html