

HIPAA REVISITED – NEW REQUIREMENTS IN THE ECONOMIC STIMULUS BILL

By Jeanine Freeman, JD

The American Recovery and Reinvestment Act of 2009 (ARRA) is the economic stimulus bill passed by Congress and signed by the President. HITECH, the “Health Information Technology for Economic and Clinical Health Act,” is that portion of the ARRA calling for a nationwide system of health information technology (HIT). Despite unabashed excitement for HIT, lawmakers are concerned that patient privacy could be more easily compromised in an electronic system. Too, some believe that HIPAA has not been enforced. As such, HITECH includes several new HIPAA privacy and security requirements. The effective date for most changes is 12 months from February 17, 2009, ARRA’s enactment date. Many questions exist, e.g., do HITECH’s provisions apply only to electronic medical record systems? Regulations will provide guidance but time for compliance may be short.

Terminology. HITECH adds definitions to existing HIPAA law and regulations for “electronic health record (EHR),” “personal health record (PHR),” “PHR vendor,” “breach,” and “unsecured PHI (protected health information).” A PHR is electronically held identifiable health information drawn from multiple sources and managed and controlled by or primarily for the individual; a PHR is not the same as the provider’s medical record. “Unsecured” PHI is patient-identifiable medical information that is not encrypted. “Breach” is the unauthorized acquisition, access, use, or disclosure of PHI that compromises its security or privacy; exceptions are provided.

Business associates. HIPAA now regulates business associates (BA) of covered entities (CE) through HIPAA-compliant agreements the CE enters into with the BA. Under HITECH,

CEs still will have agreements with their BAs reflecting HIPAA requirements but BAs also will be directly bound by HIPAA and subject to civil and criminal sanctions for HIPAA violations.

TPO modifications. HIPAA now gives special address to release of PHI for purposes of “treatment, payment and healthcare operations (TPO).” HITECH makes some changes. A provider is required to honor a patient’s request to not release PHI to the patient’s health plan so long as the patient fully pays out-of-pocket for that medical service. Further, HITECH requires release of PHI consistent with its newly-defined “minimum necessary” standard even for TPO unless for treatment purposes. Also, covered entities that use EHRs are required to account for all disclosures, including TPO-related ones, effective no earlier than January 1, 2011.

Notice of breach. HITECH goes into much detail on when a “breach” of PHI occurs and required processes for disclosure of that breach. If 10 or more patients are affected, notice must be provided on the physician’s Web site; if 500 or more are affected, the media must be notified.

Marketing/sale of PHI. A CE or BA cannot receive remuneration in exchange for PHI unless the patient authorizes it or an exception applies. Regulations are to be adopted within 18 months, with compliance expected 6 months after that. HIPAA’s marketing rules also are affected.

Tougher penalties and enforcement. Civil monetary penalties for disclosure breaches range from \$100 per violation not to exceed \$25,000 per calendar year to \$50,000 per violation, not to exceed \$1.5 million per calendar year. State attorneys general are given enforcement authority over HIPAA violations.



Jeanine Freeman, JD, is Senior Vice President of Legal Affairs for the Iowa Medical Society.