

# New HIPAA/HITECH Compliance Deadline of September 23, 2013

by Gary S. Young on August 27, 2013

Are you aware that there is a compliance deadline set for September 23, 2013 that may apply to your business? When originally passed, the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) introduced new rules regarding the use and disclosure of a patient’s personal health information (“PHI”). Over the years, unless your business was directly involved in providing healthcare services, HIPAA compliance probably was not on your compliance radar. A law passed in 2009 and known as “HITECH” will now change that perspective for some businesses.

To better understand HIPAA’s application, it is important to understand some important terms:

“Personal Health Information” (“PHI”) is defined to be any health information of an identifiable individual that is transmitted by electronic media, maintained in any electronic medium or transmitted or maintained in any other form or medium. For example, all administrative, financial, and clinical information on a patient is deemed to be PHI. Any information that identifies who the health-related information belongs to (i.e. names, email addresses, phone numbers, medical record numbers, photos, drivers license numbers, etc.) is also PHI. “ePHI” is merely PHI that is stored or transmitted electronically (i.e. via email, text message, web site, database, online document storage, electronic FAX, etc.).

“Covered Entities” include:

- Health plans: With certain exceptions, an individual or group plan that provides or pays the cost of medical care.
- Health care clearinghouses: An entity that either processes or facilitates the processing of health information from various organizations, i.e. to reformat or process the data into standard formats.
- Health care providers: Care, services, or supplies related to the health of an individual, including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedures with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and (2) the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

“Business Associates” are entities (other than a Covered Entity's workforce) who store and exchange PHI data via computers through intranets, Internet, dial up modems, DSL lines, T-1, etc. and who create, receive, maintain or transmit PHI on behalf of a Covered

Entity to perform certain enumerated functions, including claims processing, data analysis, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services and data transmission services if routine access to data is required; and subcontractors of Business Associates.

HIPAA also sets Privacy and Security Rules that focus on information safeguards and requires Covered Entities to implement all necessary and appropriate means to secure and protect PHI. Specifically, these rules impose organizational and administrative requirements along with technical and physical safeguards. HIPAA's Privacy Rules set standards for protecting the rights of individuals (patients). Individuals are assured the right to PHI privacy and confidentiality. Further, PHI is subject to restrictions on proper use and disclosure. This extends to securing more reliable information systems to protect ePHI from being lost or hacked.

The Health Information Technology for Economic and Clinical Health Act ("HITECH") is part of the American Recovery and Reinvestment Act of 2009 (ARRA) which provides specific incentives designed to accelerate the adoption of electronic health record (EHR) systems among Health Care Providers. HITECH will soon extend HIPAA compliance requirements to all Business Associates, including Business Associates of Business Associates.

Before HITECH, privacy and security requirements were imposed on Business Associates through agreements with Covered Entities. HITECH and recent "Omnibus Rules" will now directly require Business Associates to comply with HIPAA Privacy and Security Rules or face penalties of \$100 to \$50,000 per violation.

Among other things, Business Associates must execute Business Associate Agreements ("BAAs") agreeing to comply with the Privacy and Security Rules by September 23, 2013 (this may be extended to 2014 where there is a BAA already in place). The Omnibus Rules will also require Covered Entities to execute BAAs with certain entities that were not previously considered to be Business Associates, such as data storage companies and other entities that provide data transmission services requiring access to the data on a routine basis.

BAAs often present model language prescribed by the government. Business Associates should consider the inclusion of additional or alternative terms that minimize legal exposure, such as:

- Prohibiting Covered Entities from asking the Business Associate to take any action that would violate the HIPAA Rules.
- Authorizing termination of the BAA if the Covered Entity agrees to new restrictions that materially harm the Business Associate's ability to perform or costs of performance.

- Alternatively, permitting the Business Associate to recover costs associated with such additional restrictions or requirements.
- Eliminating or limiting any proposed insurance or indemnification agreements.
- Waiving or limiting damages.

These suggestions are just for starters. As things inevitably evolve, Covered Entities and Business Associates should be reviewing the law's requirements and managing the risks that the law creates. For now, meeting the September 23<sup>rd</sup> deadline, if applicable, must be the first goal.

If you have any questions about the compliance deadline or would like to discuss the legal issues involved, please contact me, Gary Young, or the Scarinci Hollenbeck attorney with whom you work.