

By Stephen W. Bernstein and Edward G. Zacharias



Stephen W. Bernstein is a Partner and Firmwide Head of McDermott Will & Emery's Health Industry Practice Group.



Edward G. Zacharias is an Associate in McDermott Will & Emery's Health Industry Practice Group and served as a member of the BBA's Public Interest Leadership Program from 2008-2009.

Why Massachusetts Should Care about the HITECH Act

The Health Information Technology for Economic and Clinical Health Act (American Recovery and Reinvestment Act of 2009, H.R. 1, 111th Cong., § 13001, et seq. (Feb. 17, 2009), hereinafter the "Act") includes at least \$20 billion in government funding for health information technology. This money is intended, in part, to facilitate the development of a national health information network. To protect information as it moves through the envisioned national system, the Act significantly modifies the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191 (Aug. 21, 1996), hereinafter "HIPAA") and imposes a national security breach notification law upon entities that possess protected health information ("PHI"). The Act requires covered entities, business associates (including lawyers and law firms in certain circumstances), vendors of personal health records ("PHR") and certain third-party service providers to notify individuals and/or entities when unsecured PHI or unsecured PHR-identifiable health information is subject to a security breach.

The Act's security breach notification requirements are particularly salient in Massachusetts, where the healthcare industry is responsible for nearly 16% of the state's total employment and ranks second in the nation in grants from the National Institutes of Health. Given the scope and economic impact of the Commonwealth's healthcare industry and the push toward national health reform, the privacy and security of PHI and PHR will continue to require the attention of a large sector of the Massachusetts economy. Moreover, as healthcare spending remains front and center in our national policy debate, there is a continued focus on the delivery of high-quality, effective care as a means of combating rising costs. Analyzing patient data and measuring outcomes are vital to establishing quality metrics necessary to reduce healthcare spending. Accordingly, Massachusetts can expect the volume and the rate of exchange of health information to increase, making it crucial to address privacy and security issues.

The Act defines a security breach broadly to include the unauthorized acquisition, access, use or disclosure of PHI that compromises its security, privacy or integrity. In the event of a breach, entities subject to the Act are required to notify the individual whose information is subject to the breach, other entities responsible for the information and/or certain federal agencies, depending on the circumstances. Notices are subject to specific content, timing and form requirements.

As directed by the Act, both the U.S. Department of Health and Human Services ("HHS") and the Federal Trade Commission ("FTC") issued regulations governing the notification requirements in the event of a security breach. The HHS regulations (74 Fed. Reg. 42740 (Aug. 24, 2009)) exempt from the breach notification requirements covered entities and business associates using specific encryption and destruction technologies and methodologies that render PHI "unusable, unreadable or indecipherable". The FTC regulations (74 Fed. Reg. 42962 (Aug. 24, 2009)) are applicable to vendors of PHRs and related entities, and require such entities to notify individuals when the security of their unsecured PHR-identifiable health information is breached.

Complicating matters further, Massachusetts imposes its own set of comprehensive laws addressing data security and breaches of the “personal information” of Massachusetts residents (Mass. Gen. Laws ch. 93H; 201 Mass. Code Regs. §§ 17.00 – 17.05). Like the federal law, Massachusetts also requires affected individuals to be notified. While the HHS and FTC regulations note that contradictory state laws are preempted by the federal rules, state laws imposing breach notification requirements in excess of those required under federal law are not preempted. While the Act is broader than the Massachusetts law in the sense that PHI captures more than the Commonwealth’s definition of personal information, the risk assessment required under the HHS regulations is flexible and only requires business associates and covered entities to notify affected individuals where the breach

“poses a significant risk of financial, reputational, or other harm to the individual.” It should be noted, however, that on October 1, 2009 six Congressmen sent a letter to the Secretary of HHS, Kathleen Sebelius, indicating their concern that the significant risk of harm requirement is inconsistent with Congressional intent and sets too high of a threshold to trigger a notification requirement. It is unclear what action HHS will take to address these concerns, if any.

Compliance with these laws will require the expenditure of significant time and resources. Accordingly, Massachusetts entities subject to the Act (including many lawyers and law firms) should begin immediately familiarizing themselves with the Act, the regulations and the Massachusetts law, and updating their processes and procedures accordingly. ■

The Boston Bar Association Salutes Its Sponsors Helping Us Advance Our Mission

Anderson & Kreiger LLP
 Bingham McCutchen LLP
 Blue Cross & Blue Shield of Massachusetts, Inc.
 Boston Medical Center
 Boston Redevelopment Authority
 Brown Rudnick LLP
 Burns & Levinson LLP
 Choate, Hall & Stewart LLP
 Committee for Public Counsel Services
 Conn Kavanaugh Rosenthal Peisch & Ford, LLP
 Davis, Malm & D’Agostine, P.C.
 Day Pitney LLP
 Dechert LLP
 DLA Piper LLP (US)
 Donnelly, Conroy & Gelhaar, LLP
 Duane Morris LLP
 Dwyer & Collora, LLP
 EMC Corporation
 Foley Hoag LLP
 Gesmer Updegrave LLP
 Goodwin Procter LLP
 Goulston & Storrs – A Professional Corporation
 Greater Boston Legal Services
 Greenberg Traurig LLP
 Hanify & King, P.C.
 Hemenway & Barnes LLP
 Hinckley, Allen & Snyder LLP
 Hirsch Roberts Weinstein LLP
 Holland & Knight LLP
 Lawyers’ Committee for Civil Rights Under Law
 of the Boston Bar Association
 Legal Advocacy and Resource Center
 Looney & Grossman LLP

Massachusetts Department of Environmental
 Protection
 Massachusetts Office of the Attorney General
 McDermott Will & Emery LLP
 Michaels, Ward & Rabinovitz, LLP
 Mintz Levin Cohn Ferris Glovsky & Popeo P.C.
 New England Law | Boston
 Nixon Peabody LLP
 Nutter McClennen & Fish LLP
 Office of the Corporation Counsel,
 City of Boston Law Department
 Ogletree, Deakins, Nash, Smoak & Stewart, P.C.
 Partners HealthCare
 Peabody & Arnold LLP
 Pepe & Hazard LLP
 Rackemann, Sawyer & Brewster
 Robins, Kaplan, Miller, & Ciresi L.L.P.
 Robinson & Cole LLP
 Ropes & Gray LLP
 Ruberto, Israel & Weiner, P.C.
 Sherin and Lodgen LLP
 Shilepsky O’Connell Hartley LLP
 Skadden, Arps, Slate, Meagher & Flom LLP
 & Affiliates
 Sugarman, Rogers, Barshak & Cohen, P.C.
 Sugarman & Sugarman, P.C.
 Sullivan & Worcester LLP
 Sunstein Kann Murphy & Timbers LLP
 Todd & Weld LLP
 Verrill Dana LLP
 Weil, Gotshal & Manges LLP
 Wilmer Cutler Pickering Hale and Dorr LLP
 Yurko, Salvesen & Remz, P.C.

Professional Excellence

Facilitating Access to Justice

Serving Our Community

Reprinted with Permission from the Boston Bar Journal,
a Publication of the Boston Bar Association.