

Protecting the Privacy of Patient Information Under the Health Information Technology for Electronic and Clinical Health Act (HITECH Act)

May 2009

EVELYN A. HARALAMPU

is a Partner and heads the ERISA, employee benefits and executive compensation practice of the Firm.



On February 17, 2009, the American Recovery and Reinvestment Act of 2009 (the stimulus package) was signed into law. Part of that package, the Health Information Technology for Economic and Clinical Health Act (HITECH Act), significantly expands the scope of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It adds stringent penalties for infractions relating to the privacy protection of patients' health information, and extends the legal requirements of HIPAA to business associates of healthcare providers and other covered entities as well as to vendors of personal health records and health information exchange organizations. The HITECH Act encourages the encryption of protected health information by imposing significant penalties for the unauthorized disclosure of unprotected health information and imposes a new, mandatory disclosure requirement in the event of breaches relating to health information.

DISCLOSURE REQUIREMENTS

HIPAA does not require health care providers and other covered entities to notify patients of any unauthorized disclosures of their protected health information. Formerly, such disclosures were made in accordance with applicable state security breach notification laws and general legal principles to mitigate harm that could result from the

unauthorized use or disclosure of protected information. The HITECH Act adds to the application of these legal principles by imposing mandates that patients be notified in certain circumstances of the unauthorized acquisition, access, use, or disclosure of their unsecured protected health information that compromises the privacy or security of that information. The HITECH Act also requires business associates that discover a breach in the security of unprotected health information to notify the covered entity to which they provide services. That notification must be made without unreasonable delay and in no case later than 60 days after discovery of the privacy breach. The unauthorized use of protected health information may also be subject to regulation under Massachusetts laws that governs the disclosure of the personal information of Massachusetts residents. However, the more stringent requirements of the federal law will generally take precedent.

The notification requirements of the HITECH Act relate to "unsecured protected health information". Unsecured protected health information is generally information that is not secured by a technology standard that renders it unusable, unreadable or undecipherable to unauthorized individuals and is developed or endorsed by the American National Standard Institute. If a breach affects 500 patients or more it must be reported to Health and Human Services (HHS), which will post the name of the breaching entity on its website, and offer steps that individuals should take to protect themselves from potential harm. Breaches affecting 500 patients or more who reside in the same area must be reported to the local media as well.

BUSINESS ASSOCIATES

Business Associates serving healthcare providers and other covered entities are now subject to additional requirements relating to the protection of patient information. These new obligations must be incorporated into the business associate agreements with covered entities. For example, business associates, like covered entities, are now required either to correct a pattern of activities or practice that violates the privacy obligations, terminate the contract with the covered entity or report the problem to HHS.

Business associates must also comply with the administrative, physical and technical safeguards under the HIPAA Security Rule regarding the protection of health information. They are also subject to civil and criminal penalties for their own violations as well as the violations of a covered entity which the business associate serves if the business associate is aware of those violations and does not take steps to correct or mitigate them.

ENFORCEMENT, PENALTIES AND AUDITS

Civil penalties against business associates and covered entities are assessed based on the level of intent and neglect involved. For violations of the HITECH Act made without knowledge the penalties start at a \$100 per violation and are capped at \$25,000. For violations based on "reasonable cause", penalties start at \$1,000 per violation and are capped at \$100,000. For violations due to willful neglect, penalties start at \$10,000 and are capped at \$250,000. For violations due to willful neglect that are not corrected, penalties start at \$50,000 and are capped at \$1.5 million. The HITECH Act imposes

• continued

mandatory penalties for violations that are due to willful neglect, and also requires HHS to investigate complaints of violations by companies that are potentially neglecting the obligations of the law willfully. In addition, the HITECH Act clarifies that criminal penalties may apply to an individual or employee of a covered entity that obtains protected health information without authorization.

The HITECH Act allows the Office of Civil Rights (OCR) to continue to use corrective action without a penalty but only in situations where the violation was made without knowledge.

While HIPAA does not provide a private right of action for patients, the HITECH Act authorizes state attorneys general to file suits on behalf of the residents.

The HITECH Act also requires HHS to conduct periodic audits of both covered entities and business associates to insure HIPAA compliance.

STEPS TO TAKE

The following are some important strategies for covered entities and business associates to take for complying with the new HITECH Act requirements:

- Identify whether protective health information that your organization handles is unsecured. More governmental guidance on the definition of “unsecured health information” is forthcoming.

- Review and amend your organization’s business associate agreements to reflect the requirements of the HITECH Act. Make sure the business associate agreement protects your organization if the other party breaches its obligations.
- Develop written policies and procedures for the use of protected health information by your organization’s employees, agents, business associates and other entities.

Evelyn Haralampu, Partner

Evelyn Haralampu heads Burns & Levinson’s employee benefits/ERISA and executive compensation practice. She is also a member of the Tax, Corporate, Private Client and Labor, Employment and Employee Benefits Groups. Ms. Haralampu has extensive experience advising both businesses and non-profit entities. In particular, she counsels on employee benefits design, executive compensation programs, equity-based compensation, health care privacy, employment law, and tax related issues.

About Burns & Levinson

Burns & Levinson, with over 120 attorneys in four offices in New England, is a full-service Boston-based law firm. The firm has grown steadily and strategically throughout the years and has become a premier law firm with regional, national and international clientele. The firm has expertise in corporate law, finance, venture capital, private equity, tax, bankruptcy, lending and leasing, real estate, business litigation, government investigations and white collar crime defense, intellectual property - including patent law, and a large private client group – including estate planning, probate and trust litigation, divorce and other family law issues. In addition, the firm has a wholly-owned subsidiary office in Montreal, Quebec, to service its Canadian clients. For more information, visit Burns & Levinson at burnslev.com.

Massachusetts Offices
Boston (HQ) 617.345.3000
Hingham, Waltham

Rhode Island Office
Providence 401.831.8330

BURNS & LEVINSON LLP
burnslev.com

This Client Update provides general information and does not constitute legal advice. Attorney Advertising. Prior results do not guarantee a similar outcome.
© 2009 Burns & Levinson LLP. All rights reserved.