

PRACTICAL ADVICE

FROM THE HEALTH LAW DEPARTMENT



Fox Rothschild ^{LLP}
ATTORNEYS AT LAW

HITECH ACT GREATLY EXPANDS HIPAA'S SCOPE: UNDERSTAND THE AMENDMENTS - ADDRESS THE CHANGES

The American Recovery and Reinvestment Act of 2009 (the Stimulus Bill) was signed into law by President Obama on February 17, 2009. The Stimulus Bill contains substantive changes to HIPAA privacy and security rules as part of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The Stimulus Bill's impact on HIPAA has raised many questions regarding changes to HIPAA security and privacy and enforcement and non-compliance risk. Many are asking what the changes mean for their businesses and what should businesses be doing to ensure compliance. In order to help clarify issues such as new privacy requirements, civil penalties and other significant changes, Fox Rothschild has assembled a cross-functional team that can assist clients in addressing and planning for new and expanded obligations.

WHO IS AFFECTED?

The HITECH Act will have a significant impact on not only those entities that were previously covered under HIPAA, namely health care providers, health plans and health care clearinghouses (a.k.a. covered entities), but also on HIPAA business associates and vendors of personal health records (PHRs), who now have direct privacy and security compliance obligations and can be assessed penalties for noncompliance.

WHAT HAS CHANGED ABOUT HIPAA?

1. **Security Breach Notification:** Covered entities, business associates and vendors of PHRs will now be required to abide by specific security breach notification requirements, including sending a written notice to affected individuals and potentially notifying the Secretary of Health and Human Services (HHS) or the Federal Trade Commission or the media if more than 500 individuals of a particular state are affected.
2. **Patient Access Rights Extended:** Covered entities that use or maintain electronic health records (EHRs) will now be required to provide patients with protected health information (PHI) in an electronic format upon request and, if the individual chooses, to transmit such copy directly to any entity or person designated by the individual.
3. **Accounting Disclosures Through Electronic Health Records:** Covered entities that use and disclose e-PHI through EHRs will need to track all uses and disclosures, including for treatment, payment and health care operations, and provide an accounting of disclosures upon a patient's request. Accounting for disclosures may begin as early as

January 1, 2011, dependent on when the entity acquires and begins to use an EHR.

4. **Complying with Requested Restrictions:** If individuals request a restriction on disclosures of their PHI to a health plan for purposes of carrying out payment or health care operations and the PHI pertains to an item or service for which the provider has been paid out-of-pocket in full, this requested restriction must be honored.
5. **No Sale of PHI:** The HITECH Act now expressly prohibits direct or indirect receipt or remuneration in exchange for any PHI without prior written valid authorization, except in a very limited number of circumstances.
6. **Marketing:** Activities that previously were viewed as "health care operations" may now be subject to HIPAA marketing restrictions.
7. **Fund-raising:** The HITECH Act tightens requirements for fund-raising communications to require that an opportunity to "opt-out" is presented in a clear and conspicuous manner.
8. **Further Guidance on "Minimum Necessary" and "Health Care Operations"** is urged and due out before February 17, 2010.

WHAT ARE THE NEW PENALTIES FOR ENFORCEMENT?

1. **Increased Civil Penalties for HIPAA:** Civil penalties for violation of HIPAA privacy and security rules will now range from \$100 to \$50,000 per offense, with penalties for additional violations within a year ranging from \$25,000 to \$1.5 million. The new provisions are effective immediately for all violations occurring from and after the date of enactment of the HITECH Act.
2. **HHS Audits and Investigations:** HHS is now required to investigate complaints and impose penalties for willful neglect.
3. **State Attorney General Enforcement Authority:** State attorneys general are now given new civil enforcement authority related to violations of HIPAA and the HITECH Act, which will result in increased investigations of complaints and enforcement.
4. **New Financial Incentives for Individuals To Report HIPAA Violations:** Beginning in February 2012, HHS will establish regulations that will allow a portion of the collected civil money penalties to be distributed to anyone whose PHI was improperly used or disclosed.

(Continued)

HOW CAN FOX ROTHSCHILD HELP?

Fox Rothschild attorneys have extensive experience with privacy and security compliance including:

- Developing HIPAA assessment tools, checklists, policies, procedures and training programs for our clients;
- Assisting all types and sizes of health care providers in preparation of license agreements, consent forms and other legal documentation in connection with implementation of EHRs, PHRs and EMRs, as well as for participation in health information exchanges (HIEs) and regional health information organizations (RHIOs);
- Providing analysis to synchronize state requirements with federal privacy and security requirements; and
- Participating with federal and state privacy and security committees and collaborations, such as HISPC and the NJ Health Information Technology Commission.

We are aware of the amendments the HITECH Act has made to HIPAA's privacy and security requirements and are ready to guide our clients through the maze of changes that have and will continue to occur through regulation in this area. Services we offer include:

- Checklists and tools, such as the "HITECH Deadlines Calendar," to help clients comply with the various requirements to be phased in over the next 18 months;
- Updating Notice of Privacy Practices;
- Updating privacy and security policies and procedures;
- Developing a detailed Breach Notification Policy that complies with the new federal breach notification provisions and any state law counterpart;
- Updating Business Associate Agreements to include new requirements;
- Developing any new documentation required under the HITECH Act, such as the "Breach Log" to be submitted to the Secretary of HHS annually; and
- Reviewing any EHR subsidy programs between hospitals and physicians, among other types of services.

For general information regarding legal developments that providers and businesses must consider with regard to the handling and sharing of health information, visit the HIPAA, HITECH & HIT Blog <http://hipaahealthlaw.foxrothschild.com>.



Fox Rothschild LLP

ATTORNEYS AT LAW

www.foxrothschild.com

© 2012 Fox Rothschild LLP. All rights reserved. This publication is intended for general information purposes only. It does not constitute legal advice. The reader should consult with knowledgeable legal counsel to determine how applicable laws apply to specific facts and situations. This publication is based on the most current information at the time it was written. Since it is possible that the laws or other circumstances may have changed since publication, please call us to discuss any action you may be considering as a result of reading this publication.

THE FOX ROTHSCHILD TEAM

Michael Kline (mkline@foxrothschild.com)

Michael counsels and assists hospitals, nonprofit foundations, skilled nursing facilities, and others in handling overlapping business, financial, governance and legal issues. He is responsible for starting and developing the firm's HIPAA experience back in 2001 and continues to stay abreast of cutting edge developments in privacy and security issues in health care, as well as the interrelationships with governance and compliance issues of institutional providers. For over 25 years, he has served as general counsel to Deborah Heart and Lung Center and Deborah Hospital Foundation in Browns Mills, NJ.

Elizabeth Litten (elitten@foxrothschild.com)

Elizabeth focuses her practice on New Jersey regulatory issues with a concentration in health law, corporate and government relations. She has been a health law attorney for more than 20 years and a registered NJ lobbyist for more than 15 years, working closely with the executive and legislative branches in developing health care policy. Elizabeth represents New Jersey hospitals, physicians, ambulatory care facilities and other New Jersey-licensed providers and health care carriers on a wide spectrum of managed care, certificate of need, licensing, reimbursement and compliance issues. In the area of health information technology, she has provided advice regarding development and implementation of HIT and has served as co-chair of the State Law Solutions subcommittee and as a member of the Electronic Health Information workgroup of the New Jersey Health Information Security and Privacy Collaboration.

William Maruca (wmaruca@foxrothschild.com)

William Maruca has extensive experience in representing physicians in Medicare and Medicaid compliance, the Stark Physician self-referral law, the False Claims Act, and federal and state regulatory requirements, including HIPAA. He represents all types of health care clients ranging from physician practices to hospital systems.

Steven Ludwig (sludwig@foxrothschild.com)

Keith McMurdy (kmcmurdy@foxrothschild.com)

Steven represents clients in the full range of labor and employment matters, including HIPAA regulatory compliance. Keith represents benefit plans, plan sponsors, plan administrators and insurers and provides counseling on compliance issues for applicable federal and state regulations.

Alan Wohlstetter (awohlstetter@foxrothschild.com)

As chair of the firm's Infrastructure Practice, Alan represents a variety of clients involved in infrastructure projects with a focus on transportation, education and information technology.

For more information, please contact any member of our team or visit us on the web at www.foxrothschild.com.