

New HIPAA Regulations Place Providers at Significant Risk

Earlier this year, the stimulus package passed by the Federal government, known as the American Recovery Reinvestment Act of 2009 (ARRA), contained provisions known as the “Health Information Technology for Economic and Clinical Health Act” (HITECH). HITECH’s provisions, signed into effect on February 17, 2009, included sections that significantly revised the “Health Insurance Portability and Accountability Act of 1996” (HIPAA).

NEW Breach Notification Provisions

Under HITECH, covered entities must notify individuals whose Protected Health Information (PHI) has been improperly disclosed because of a breach. Moreover, their Business Associates (any third party with whom a provider shares patient PHI for purposes of treatment, operations or payment), must advise a Covered Entity of any breach so that the Covered Entity may promptly notify an affected individual.

Both Covered Entities and Business Associates must make notifications no later than sixty calendar days after the breach’s discovery. The notice of breach must include:

- A brief description of what happened, when the breach occurred and when it was discovered.
- A description of what was disclosed in the breach.
- The steps individuals should take to protect themselves from potential harm resulting from the breach.
- A brief description of what the Covered Entity is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, website, or postal address.

Heightened Penalties Under HIPAA

HITECH will enhance civil financial penalties for violations. A tiered schedule applies as set out below:

- \$100 for each violation where the breach was not known even by exercising reasonable diligence, up to \$25,000 per year for identical violations.
- \$1,000 for each violation due to reasonable cause but not willful neglect, up to a maximum of \$100,000 per year for identical violation.
- \$10,000 for each violation due to willful neglect that is corrected in a timely manner, up to a maximum of \$250,000 per calendar year for violation of the same requirement.
- \$50,000 for each violation due to willful neglect if not corrected in a timely manner, up to a maximum of \$1,500,000 per calendar year for violation of this type.

Recoveries by Affected Individuals

Affected individuals may be allotted a portion of a civil monetary penalty or settlement collected by HHS. While interim regulations covering the specific actions to be taken have not been published, Business Associates should expect requirements of notifying covered entities of a breach and take remedial efforts to minimize any adverse effects caused by the improper disclosure.

New Patient Rights

HITECH grants individuals several new rights regarding protected health information including but not limited to:

- Covered entities must honor an individual's request not to share information with his / her health plan for payment or health care operations if the individual is paying the full cost of the service to which the information relates.
- Covered entities storing electronic health records will now be required to give individuals copies of their records.
- Covered entities maintaining electronic health records, at the individual's request, are obligated to provide an accounting of all disclosures of the individual's protected health information made for treatment payment and health care operations during the prior three years.
- Fundraising communications must notify individuals that they have a right to opt out of any future fundraising solicitations.

With the implementation of the HITECH Act, it is now more important than ever that health care providers and their Business Associates take significant, effective precaution to prevent the improper dissemination of unsecured PHI. Covered Entities and Business Associates now face significant penalties when breaches occur. We strongly recommend that health care providers take appropriate steps to reduce the likelihood of a breach. These include, but not limited to:

- Revise your current Compliance Plan, policies and procedures to incorporate the new obligations imposed on both health-care providers (as a Covered Entity) and their Business Associates.
- Conduct training with your staff to better ensure that everyone in your organization recognizes the importance of complying with HIPAA's expanded enforcement, breach and notification provisions.
- If you have not already done so, examine each of your third-party relationships with whom you properly disclose PHI to ensure that updated Business Associate Agreements are in place.

This article was furnished courtesy of Liles Parker PLLC and Practice Management Institute. This content has been provided as general information only. It does not constitute legal advice and should not be used as a substitute for seeking legal counsel. Readers with legal questions should call Liles Parker PLLC or consult their attorney.

Publications related to this topic on website www.practicesupport.com include:

[HIPAA Compliance Manual](#)

[HIPAA Handbook for Physicians: Understanding the Privacy & Security Regulations](#)

