



Health Care Law Information Memo

March 2010

Electronic Dispatch

[Go to BS&K Health Care Law Home Page](#)

BREACH NOTIFICATION REQUIREMENTS: HIPAA, THE HITECH ACT, AND NEW YORK LAW

On February 22, 2010, covered entities became subject to sanctions by the United States Department of Health and Human Services (HHS) for noncompliance with the HIPAA breach notification rule. As covered entities and business associates take steps to implement compliance with the new rule, they should also evaluate their policies and procedures for compliance with notice requirements under § 899-aa of the New York General Business Law.

“Breaches” under the HITECH Act

New HIPAA compliance challenges for covered entities and business associates were created by the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). Enacted in 2009 as part of the American Recovery and Reinvestment Act, the HITECH Act expanded the scope of HIPAA enforcement and created a requirement that covered entities notify affected individuals when certain violations of the HIPAA Privacy Rule occur.

Not every violation of the HIPAA regulations is a “breach” that triggers an obligation to notify affected individuals. For purposes of the HITECH Act, a “breach” has occurred if unsecured protected health information (PHI) has been acquired, accessed, used, or disclosed in a manner that (1) violates the HIPAA Privacy Rule, and (2) poses a significant risk of financial, reputational, or other harm to the individual. The breach notification regulations promulgated by HHS contemplate that the covered entity will conduct a risk assessment to evaluate whether the Privacy Rule violation poses a significant risk of financial, reputational, or other harm.

If the violation poses such a risk, affected individuals must be notified without unreasonable delay, and in no case later than 60 days after the covered entity knew of the breach or would have known of it by exercising reasonable diligence. The method and content of notice are defined in the HHS regulations.

The obligation to notify affected individuals falls on the covered entity, even if the breach is discovered by or caused by its business associate. The business associate’s obligation is to notify the covered entity of breaches on a timely basis.

When a breach involves PHI of 500 or more individuals, the covered entity is required to concurrently notify prominent local media outlets and HHS. For breaches involving PHI of fewer than 500 individuals, the covered entity is required to maintain a log and file an annual report with HHS. Summary information on breaches concerning 500 or more individuals is posted by HHS on its Office for Civil Rights website.

Notification requirements under New York law

Entities doing business in New York State must also comply with notification obligations under § 899-aa of the General Business Law. Since 2005, this statute has required businesses to notify affected New York residents when loss of or unauthorized access to certain types of unencrypted computerized data occurs.

In contrast to the HITECH Act, which pertains only to PHI, the reporting obligations under GBL § 899-aa arise only when the compromised computer data includes individually identifiable Social Security numbers, driver’s license numbers, or financial account numbers with access codes. When unencrypted computerized data that includes any of these data elements is compromised, the business is required to notify affected New York residents by the methods prescribed in the statute. In addition, the entity must notify the New York State Attorney General’s Office, the New York State Office of Cyber Security & Critical Infrastructure Coordination, and the New York State Consumer Protection Board.



There is some potential overlap between the breach notification obligations under the HITECH Act and the notification requirements under New York law, and an event that implicates one statute may or may not implicate the other. Both statutes should be considered when assessing an incident that involves loss of patient information in electronic format.

Review policies and procedures

In order to comply with the federal and New York State notification requirements, covered entities and business associates should incorporate incident identification and breach reporting into their HIPAA privacy and security compliance policies and procedures. Risk assessment and breach notification should be coordinated with a covered entity's policy and procedure for mitigation of known harmful effects of Privacy Rule violations.

At the same time, a covered entity should evaluate its policies and procedures on individual rights to ensure that they are current. Although the HIPAA Privacy Rule allowed individuals to request restrictions on disclosure of their PHI, the covered entity was not required to honor such requests. Under the HITECH Act, a covered entity must now abide by an individual's request not to disclose PHI to a health plan, if the PHI pertains solely to a health care item or service for which the provider has been paid out-of-pocket and in full.

Review business associate agreements

The HITECH Act does not necessarily require covered entities to update their business associate agreements, and HHS has not issued any guidance on existing business associate agreements. Under the HIPAA Privacy Rule, the required elements for business associate agreements have always included the business associate's commitment to notify the covered entity of unauthorized uses and disclosures of PHI. That obligation is broad enough to encompass the breaches of unsecured PHI that the business associate is now required to disclose to the covered entity under the HITECH Act.

Although the business associate's obligation to inform the covered entity of improper disclosures is not new, and business associate agreement updates are not mandated by regulation, covered entities and their business associates should nonetheless review business associate agreements in light of the HITECH Act. For example, the parties may wish to consider whether their contracts should be revised to address the costs that would be involved in notifying individuals of a breach.

Future developments

With further regulations implementing other aspects of the HITECH Act yet to be issued, HIPAA compliance will be an evolving process. Covered entities and their business associates will need to stay abreast of changes, with due regard for higher penalty exposures and increasingly stringent enforcement.

If you have any questions, please contact:

In Buffalo / Niagara Falls, call 716-566-2800 or e-mail:

Robert A. Doren rdoren@bsk.com

In the Capital District, call 518-533-3000 or e-mail:

Hermes Fernandez hfernandez@bsk.com

In Central New York, call 315-218-8000 or e-mail:

Larry P. Malfitano lmalfitano@bsk.com

Patrick J. Pedro ppedro@bsk.com

In Garden City, call 516-267-6300 or e-mail:

Terry O'Neil toneil@bsk.com

In New York City, call 646-253-8000 or e-mail:

Louis P. DiLorenzo ldilorenzo@bsk.com

In Northern New York, call 315-218-8000 or e-mail:

Larry P. Malfitano lmalfitano@bsk.com

In the Rochester Region, call 585-362-4700 or e-mail:

Robert H. Kirchner rkirchner@bsk.com