A Timely Analysis of Legal Developments

ASAP®

In This Issue:

March 2009

Two recent enforcement actions and significant amendments to the HIPAA Privacy Rule, enacted as part of the federal government's massive economic stimulus bill (the "American Recovery and Reinvestment Act of 2009" (ARRA)), should re-focus employers on their HIPAA compliance efforts. The ARRA requires new security breach notification requirements for "unsecured" protected health information and enhanced business associate obligations under HIPAA.

Recent Enforcement Actions and Significant Amendments to the HIPAA Privacy Rule Compel Employers to Revisit Their HIPAA Compliance Efforts

By Philip L. Gordon

Two recent enforcement actions and significant amendments to the HIPAA Privacy Rule, enacted as part of the federal government's massive economic stimulus bill (the "American Recovery and Reinvestment Act of 2009" (ARRA)), should re-focus employers on their HIPAA compliance efforts. Within the past seven months, the U.S. Department of Health and Human Services (HHS) has obtained a settlement payment of $100,000 from a hospital system that suffered five reported security incidents in approximately 18 months and a $2.5 million settlement from a pharmacy chain that allegedly discarded pharmacy records without shredding or otherwise rendering the information irrecoverable. Consistent with this increased emphasis on enforcement, ARRA requires that HHS conduct "periodic" compliance audits of entities subject to regulation under HIPAA.

Such "breach-driven" enforcement is likely to become more frequent under ARRA. The ARRA provisions concerning HIPAA, effective February 17, 2010, require that employers who sponsor HIPAA-covered plans notify not only affected plan participants of any security breach caused by the employer or its service provider (referred to in HIPAA as a "business associate"), but also, if the breach involves 500 or more plan participants, notify major media outlets and HHS as well. Employers should revise their agreements with their service providers/business associates ("business associate agreements" in HIPAA parlance) to address security breach notification as well as several other amendments to HIPAA contained in ARRA.

New Security Breach Notification Requirements

While 45 states and the District of Columbia have enacted security breach notification laws, only three states — Arkansas, California, and Delaware — include "health information" among the categories of information, the unauthorized acquisition of which triggers a statutory obligation to provide notice of a security breach. The ARRA provisions *partially* close that gap. They require notice to affected individuals in the event of an unauthorized access to, or use, disclosure, or acquisition of, "unsecured" protected health information (PHI) that compromises the information's security or

privacy. ARRA does not define the term "unsecured." Instead, ARRA directs HHS to issue guidance on or before April 17, 2009, on the types of technology that would render PHI secure and, therefore, obviate the need for notice in the event of a breach. If state security breach notification laws will serve as a guide for HHS, the mandated security technology most likely will be some form of encryption.

Employers should note a critical limitation on the scope of this notice requirement. PHI, in the employment context, encompasses only those records created or received by, or on behalf of, an employer *in its capacity as the administrator of a HIPAA-covered plan*. Such plans generally are limited to self-insured group health, dental and vision plans; long-term care (but not long-term disability) plans; pharmacy benefits coverage; a health care reimbursement flexible spending account ("health FSA"); and an employee assistance program (EAP). Medical records that the employer creates or receives in its capacity as the employer — such as sick leave requests, first reports of injury, and Family and Medical Leave Act (FMLA) certifications — are *not* PHI and would not trigger a mandatory notice obligation under HIPAA if subjected to unauthorized access, use, disclosure or acquisition.

As a practical matter, most employers have only limited, if any, PHI at the worksite because they rely upon a third-party administrator to perform the administration of their self-insured health plans, health FSA and EAP. The ARRA provisions address this potential lacunae by requiring that any business associate promptly notify the employer of a breach, including an identification of each affected individual. The employer retains the legal obligation to notify affected individuals.

Affected individuals must be notified within 60 calendar days after the employer or the business associate knows, or reasonably should have known, of the breach. Significantly, the ARRA provisions do not establish a minimum time period for the business associate to notify the employer. For this reason, it is critical that employers include in their business associate agreements a provision requiring the business associate to notify the employer of any breach no later than one to three days after the breach becomes known to the business associate. Otherwise, the employer's time for providing notice will start running without the employer even being aware of the breach.

The notice to affected individuals must include, at a minimum, the following five categories of information: (1) a brief description of what happened, the date the breach was discovered, and the date the breach occurred, if known; (2) an identification by category of the PHI that was compromised, e.g., Social Security number (SSN), diagnosis, date of birth; (3) how individuals may protect themselves against possible harm resulting from the breach; (4) a brief description of the investigation, of efforts to mitigate any harm, and of steps taken to prevent a recurrence; and (5) contact information for recipients of the notice to ask question or obtain additional information. Employers should note that while the amendments do not require an offer of any service to assist affected individuals, such services, *e.g.*, credit monitoring or fraud resolution services, commonly are offered.

The ARRA provisions also establish detailed requirements for delivering the notice. The notice must be sent by first-class mail to the affected individual's last known address. If the affected individual is deceased, the notice must be sent to the individual's next of kin. If the employer possesses insufficient or out-of-date contact information, the employer must provide a substitute form of notice. If a breach requires substitute notice to ten or more individuals, the employer must post a conspicuous notice on its Web page or post a notice in the media. Avoiding the need to provide such "substitute notice" is yet another incentive for ensuring that the employer and its business associates maintain current records and purge their files of information on plan participants when no longer needed.

Notably, breaches involving more than 500 individuals will have the potential to result in substantial embarrassment and an investigation by HHS. When such breaches occur, the employer is required to notify "prominent media outlets serving a State or jurisdiction" and also must "immediately" notify HHS. HHS will identify the employer in a list posted on the agency's Web site. Employers must maintain a log of breaches involving fewer than 500 individuals and submit the log annually to the Secretary. Employers can expect that HHS will draw its audit targets at least in part from these notices and that attorneys and unions representing employees will use HHS's "breach Web site" as a possible source for action against an employer.

Enhanced Business Associate Obligations

Under the HIPAA Privacy Rule, an employer in its capacity as plan administrator must contractually require any third-party vendor who receives or creates PHI on the employer's behalf to provide certain contractual assurances concerning its handling of PHI. These

assurances typically are included in a separate agreement, the "business associate agreement" mentioned above. The new ARRA provisions will require employers to amend existing business associate agreements in several respects.

To begin with, business associates must now expressly agree that they will comply with the principal requirements of the HIPAA Security Rule. While this requirement, on its face, should demand little more than the insertion of a sentence into existing business associate agreements, employers should strongly consider doing some form of due diligence to confirm compliance by the business associate with the new provision. A business associate who pays only lip service to contract language and does not comply fully with the Security Rule will be more vulnerable to a security breach. As explained above, such breaches could result in the employer's having to incur substantial cost to provide notice to affected individuals, embarrassment from being identified in the media and on HHS' Web site as an entity responsible for a security breach involving 500 or more individuals, and an audit by HHS of the employer's HIPAA compliance efforts.

Second, as noted above, the business associate agreement should require that the business associate immediately notify the employer of any breach. The agreement should require the business associate's notice to include not only an identification of all affected individuals (as is required by ARRA) but also: (a) a brief description of the breach; (b) the date that the breach occurred; (c) the date the business associate discovered the breach; (d) the categories of PHI involved in the breach; (e) the status of the business associate's investigation; (f) the steps, if any, the business associate has taken to mitigate the harm caused by the breach; and (g) the steps the business has taken, or will take, to prevent a recurrence. The employer will need this information to prepare its notice to affected individuals.

Third, the business associate agreement should include an indemnification provision that includes all expenses incurred by the employer when responding to any security breach caused by the business associate's actions or inaction. The indemnification provisions should expressly include within its scope attorneys' fees, consultants' fees, the costs of delivering notice to individuals, the cost of any notice published in the media, the cost of services offered to affected individuals, and the cost of responding to any audit triggered by the breach. Depending upon the size of a security breach, these costs could exceed several hundred thousand dollars.

Finally, ARRA includes a provision that is fairly technical but must be addressed in the business associate agreement. Until HHS issues guidance on or before August 17, 2010, as mandated by ARRA, employers and business associates are required to limit their use and disclosure of, and requests for, PHI, to a "limited data set" unless a greater amount of PHI is the minimum necessary to accomplish the purposes of the use, disclosure or request. A "limited data set" is PHI that excludes a long list of identifiers regarding the individual, his or her relatives, employers and household members, including, for example, name, all contact information, SSN, full face photograph and health plan number. This requirement needs to be included in the business associate agreement.

Conclusion

Before ARRA's provisions concerning HIPAA become effective in February 2010, employers should revisit their own HIPAA compliance efforts, discuss with their business associates the security measures that have been implemented to reduce the risk of a security breach involving unsecured PHI, and amend their business associate agreements to address the new compliance obligations and risks created by ARRA.

Philip L. Gordon is a Shareholder in Littler Mendelson's Denver office, and Chair of Littler Mendelson's Privacy & Data Protection Practice Group. He maintains a blog on employment related privacy issues at http://privacyblog.littler.com. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com.