Morgan Lewis

alert

employee benefits lawflash

January 25, 2013

Final Rules Under HIPAA/HITECH Impact Employer Plans

Modifications to the rules require action by group health plan sponsors and their vendors, including revisions to policies and procedures and new privacy notices.

On January 17, the Office for Civil Rights of the U.S. Department of Health and Human Services (HHS) released final regulations under the Privacy Rule, the Security Rule, and the Enforcement Rule under the Health Insurance Portability and Accountability Act (HIPAA) and the Breach Notification for Unsecured Protected Health Information Rule (Breach Notification Rule) under the Health Information Technology for Economic and Clinical Health (HITECH) Act.[1]

The final rules are effective on March 26, 2013, and covered entities and business associates generally must comply with the applicable requirements by September 23, 2013. Employer group health plan sponsors and the business associates that service them will be impacted by several modifications under the new rules, as described below.

Business Associate Agreements

The final rules make business associates, such as vendors that provide services to or on behalf of group health plans, directly liable for compliance with the Security Rule and certain standards under the Privacy Rule. The definition of "business associate" has been revised to include all subcontractors of business associates that create, receive, maintain, or transmit protected health information (PHI) on behalf of a covered entity, no matter how "downstream" those subcontractors may be. Business associates are responsible for entering into business associate agreements with their subcontractors.

Employer plan sponsors should review their agreements with plan vendors to ensure that they require the business associate to (1) comply with the Security Rule and report any security breach to the covered entity, (2) comply with the Privacy Rule as it applies to obligations delegated to the business associate under the agreement, and (3) enter into a business associate agreement with each subcontractor that receives the plan's PHI that contains the same (or greater) protections as the agreement with the covered entity.

Breach Investigations

A "breach" was defined under the prior rules as an impermissible use or disclosure that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual. The final rules eliminate the "significant risk of harm" standard, which HHS deemed too subjective. Under the new definition of "breach," an impermissible use or disclosure of PHI is "presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised." The final rules require an analysis that, at a minimum, takes into account the following: (1) the nature and extent of the PHI, (2) who used or received the PHI, (3) whether the PHI was actually acquired or viewed, and (4) the extent to which the risk to the PHI was mitigated. A covered entity or business associate may choose to provide breach notification with respect to any impermissible use or disclosure of PHI and forego the risk assessment process. HHS has indicated that it will

1. View the January 17, 2013, HHS press release at http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

provide additional guidance related to risk assessments and common breach scenarios. Employer plan sponsors should review and revise, as necessary, their policies and procedures with respect to breach investigations to ensure compliance with the new risk assessment standards.

Access to PHI

The final rules expand individuals' rights to receive copies of their PHI by requiring covered entities to provide access to PHI in the electronic form and format requested by the individual, if the PHI is maintained electronically in one or more designated record sets (e.g., enrollment, payment, claims, and medical and billing records). Covered entities still have 30 days to respond to a request for PHI, even if the PHI will be sent electronically. The final rules also allow family members who were involved with a decedent's care to receive access to the decedent's PHI.

Restrictions on Disclosures

The final rules provide that if the full cost of medical care for a particular item or service is paid for by (or on behalf of) an individual out of pocket, the provider must abide by the individual's request to restrict PHI related to such care and not share it with the individual's health plan or insurer.

Authorizations Required for Marketing and Sale of PHI

Under the final rules, an individual authorization is required for communications when a covered entity receives financial remuneration from a third party in exchange for marketing the third party's product or service. Exceptions apply for the costs of labor, supplies, and postage related to refill reminders and other communications about currently prescribed drugs. Promotions of health in general and the promotion of government-sponsored programs are also permitted without authorization. The final rules also generally prohibit a covered entity or business associate from receiving direct or indirect remuneration in exchange for the disclosure of PHI, unless the covered entity or business associate has obtained authorization from the individual.

Genetic Information

The final rules prohibit most health plans from using or disclosing genetic information for underwriting purposes, as required under the Genetic Information Nondiscrimination Act of 2008 (GINA).

Notice of Privacy Practices

A number of provisions in the final rules will require changes to the notice of privacy practices required to be issued by covered entities. Health plans must post the revised notices on their websites and provide hard copies to participants at the next annual open enrollment.

Enforcement

HHS will continue to conduct random audits and investigate breach reports and complaints under HIPAA/HITECH. Violations can result in civil penalties of up to $1.5 million per year and criminal penalties of up to 10 years' imprisonment. The final rules maintain the tiered system of civil penalty amounts, based on increasing levels of culpability, that was introduced under HITECH. Also included in the final rules is a provision that allows HHS to impose a civil money penalty without exhausting informal resolution options, although this approach is likely to be limited to cases of willful neglect.

Next Steps

With the final regulations now in hand, employer group health plan sponsors should take a fresh look at their HIPAA/HITECH compliance to identify issues, fill gaps, and correct problems. The Employee Benefits Practice has developed a number of tools for employer plan sponsors, including self-audit assistance, HIPAA training, and

privacy officer assistance. For more information about our HIPAA Privacy Compliance Initiative, please visit http://www.morganlewis.com/hipaacomplianceinitiative.

Morgan Lewis will host a webinar on February 8, 2013, at 12:30 p.m. ET to discuss in detail the compliance mandates under the final regulations. Registration for the webinar is available at https://morganlewisevents1.webex.com/ morganlewisevents1/onstage/g.php?t=a&d=299993405.

Contacts

For more information about how the final HIPAA/HITECH rules will impact employer group health plans and about our HIPAA Privacy Compliance Initiative, please contact any of the following Morgan Lewis attorneys:

Pittsburgh		
Lauren B. Licastro	412.560.3383	llicastro@morganlewis.com
Philadelphia		
Georgina L. O'Hara	215.963.5188	go'hara@morganlewis.com
Chicago		
Andy R. Anderson	312.324.1177	aanderson@morganlewis.com
Saghi "Sage" Fattahian	312.324.1744	sfattahian@morganlewis.com

For information about HIPAA/HITECH compliance for the healthcare industry, including hospitals, physician groups, insurers, and health information technology companies, please contact any of the following Morgan Lewis attorneys:

San Francisco		
W. Reece Hirsch	415.442.1422	rhirsch@morganlewis.com
Heather Deixler	415.442.1317	hdeixler@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 24 offices across the United States, Europe, and Asia, Morgan Lewis provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. Our international team of lawyers, patent agents, benefits advisers, regulatory scientists, and other specialists—more than 1,600 legal professionals total—serves clients from locations in Almaty, Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Moscow, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

IRS Circular 230 Disclosure

To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein. For information about why we are required to include this legend, please see http://www.morganlewis.com/circular230.