ALERTS AND UPDATES

The New HIPAA Landscape: Enhanced Enforcement, Million-dollar Payments and Data Breach Self-Reporting Requirements Compel Compliance

March 1, 2011

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently intensified enforcement under the Health Insurance Portability and Accountability Act (HIPAA). HIPAA imposes numerous restrictions and requirements on healthcare providers, insurance plans, billing companies and business associates to these entities that handle patient-protected health information. Since the HIPAA rules went into effect in 2003, the focus of HIPAA enforcement has been on behavior modification; now, the focus has shifted to more accountability and stiffer sanctions for noncompliance.

In just one week in February 2011, HHS announced a $1 million settlement with General Hospital Corporation and Massachusetts General Physicians Organization Inc. ("Mass General") regarding "potential" HIPAA violations. Two days earlier, HHS announced a $4.3 million civil monetary penalty against Cignet Health, a Maryland insurance company, based on HIPAA violations and the company's failure to cooperate with OCR's investigation. These cases, and HHS's apparent willingness to put them in the spotlight, demonstrate the agency's newfound commitment to investigating, uncovering and imposing penalties for HIPAA violations. In addition, HIPAA's new data breach rule, requiring entities to report unsecured data breaches, is likely to makes it easier for HHS to follow up on HIPAA incidents.

Although the Mass General and Cignet Health cases included some glaring facts, it would not be prudent to dismiss them as outliers. In the Mass General case, an employee left a folder on a subway containing information on 192 patients in an infectious disease clinic, including information on patients with HIV/AIDS. The folder was never recovered, but there was never evidence that the information was inappropriately used—thus, the violations were "potential" rather than founded. The large settlement amount was based on Mass General's lax practices on taking patient information off-site and the sensitivity of the patient information in this case.

In the Cignet case, the insurance company failed to provide 41 patients with their medical records within the 30-day (and no later than 60-day) time frame. Cignet then failed to respond to OCR's request for documents and a subpoena, leading to the

imposition of civil monetary penalties. Cignet paid $1.3 million for the HIPAA violations, and $3 million in civil monetary penalties. One could contend that these incidents—the loss of a paper folder, resulting in no actual harm and the failure to provide documents within 60 days—are understandable in the hustle-and-bustle healthcare world. However, HIPAA is at its core a consumer-protection law; and thus, the patients' interests come first.

Tougher HHS Enforcement

Recent amendments to HIPAA provide that a violator can be fined per violation as little as $100, and as much as $50,000, depending on level of knowledge of the violation, whether the violation resulted from reasonable cause or willful neglect, and whether due diligence was performed. The maximum penalty in a year for a single covered entity for all violations of an identical provision is $1.5 million, not including civil monetary penalties.

A HIPAA investigation typically starts with a complaint by a patient, an employee or a surveyor. If HHS determines that the complaint may present a violation, it issues a letter to the alleged violator requesting further information to be submitted promptly. If there is evidence of a violation, HHS will attempt to enter into an informal resolution of the case, which may require corrective action or a resolution agreement. If HHS is not satisfied with the alleged violator's response, it may seek civil monetary penalties, as it did in the Cignet case. If criminal activity is suspected, HHS may turn over the matter to the U.S. Department of Justice.

The Data Breach Rule: A New Self-Reporting Requirement

In addition to notice by complaint, another way exists where a HIPAA incident may come to OCR's attention. Under the HIPAA data-breach interim final rule—effective in September 2009—HIPAA requires that covered entities report certain breaches of unsecured data (data that are not protected according to standards adopted by HHS) to individuals and HHS and, in some instances, to the media. The breach must involve a violation of a HIPAA privacy standard and must cause a significant risk of financial, reputational or other harm to the individual. Although the rule allows the entity to perform a careful assessment of the risks and harms related to a potential breach—(What kinds of data were accessed? Are the data likely to be recovered? To whom was the data disclosed?)—many entities are simply choosing to give notice when the risks and harms cannot be clearly determined.

On February 11, 2011, New York City's municipal hospital system notified 1.7 million patients of the theft of electronic files containing patient data from the truck of a records-management-services vendor. The information was protected, although

not encrypted to the standards level suggested by HHS. There has been no indication that the stolen information was accessed. The cost of responding to the breach, including providing notice; setting up a call center and providing credit reporting (which is not required by the rule), is estimated at $350 million—for a breach where no actual harm to an individual has been determined.

Conclusion

Healthcare providers, plans, billing companies and business associates may want to take steps to ensure HIPAA compliance. Entities should consider reviewing their HIPAA policies and procedures, as well as their technical, physical and security systems to ensure that their HIPAA programs are robust. In the event of an actual or suspected violation or breach, an entity should act promptly; the failure to act may cause more issues if a complaint is lodged or a survey reveals a violation. Even if a breach has to be reported, HHS will take into consideration the steps taken by the entity to respond to the breach. Many entities are enhancing their systems to encrypt information and buying added insurance to cover security breaches. These steps are not inexpensive, but may be much less expensive than the alternative—paying millions of dollars in fines, corrective actions and mandated response activities.

For Further Information

If you have any questions about this *Alert*, please contact Lisa W. Clark, any member of the Healthcare Information Technology Practice Group or the attorney in the firm with whom you are regularly in contact.