Bloomberg Law Reports® Health Law

New Era in HIPAA Privacy Enforcement? Recent Developments May Mean Greater Scrutiny Than Before

Andrew Elbon, Bradley Arant Boult Cummings LLP

In February, the Office of Civil Rights ("OCR") of the U.S. Department of Health and Human Services imposed the first-ever civil penalty on a health care provider in the amount of $4.35 million for multiple violations of patient access rights under the Health Insurance Portability and Accountability Act ("HIPAA") privacy rule. At about the same time, OCR entered into a substantial monetary settlement agreement with another health care provider over alleged violations of the HIPAA privacy rule arising from the loss of a few hundred individuals' protected health information.[1] By taking these enforcement actions, OCR has clearly signaled an increasing seriousness with respect to the enforcement of the HIPAA privacy and security rules and its willingness to impose substantial monetary sanctions. In light of these recent events, it is now more important than ever for companies to know their status under HIPAA and take all necessary actions to maintain compliance. Failure to do so risks exposure to significant (and easily avoidable) financial liability.

HIPAA Privacy and Security Basics and the HITECH Act

Under HIPAA, covered entities such as health care providers and health plans are directly liable for the failure to implement required policies and procedures or for operational failures that result in the impermissible use or disclosure of individuals' protected health information. Any information that is maintained or transmitted in electronic form (for example, via e-mail) is generally subject to regulation under the security rule. Under the HIPAA privacy and security rules, covered entities are required to establish policies and procedures to safeguard the confidentiality of individuals' protected health information. For health care providers, such safeguards must extend to the protection of patients' individually identifiable health information in the course of providing treatment. For health plans and insurers, the confidentiality of protected health information must be safeguarded in the course of providing coverage for the payment of health care treatment.

For example, covered entities have long been required to establish procedures to prevent the physical integration of an individual's protected health information records with other records that are maintained for the same individual (for example, employment records). With respect to the security of protected health information that is maintained in electronic form, covered entities have been required to take such common sense steps as establishing technical safeguards to prevent access to electronic protected health information stored on a laptop that is misplaced or stolen. Regardless of the implementation of appropriate safeguards, however, covered health plans and health care providers have always been at risk for monetary

---

penalties for the inadvertent release of individuals' health information that is not necessary for the performance of health-related functions.[2] Previously, however, as a matter of policy, HIPAA enforcement was largely driven by the investigation of complaints by individuals whose protected health information may have been misused. It would appear that is no longer the case.

In addition, following passage of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), covered entities that are at fault for the impermissible use or disclosure of individuals' protected health information face substantially greater monetary penalties. Indeed, the civil and criminal monetary sanctions that may be imposed by OCR for violations of HIPAA by either a covered entity or its business associate were dramatically increased by the HITECH Act. Currently, there are now four penalty tiers ranging from $100 to $50,000 for each violation, with $25,000 to $1,500,000 for similar violations in the same year. Penalties may vary depending on the degree of culpability of the covered entity or business associate, with the most severe penalties reserved for violations arising from what the HITECH Act calls "willful neglect."

The HITECH Act also introduced new ways for HIPAA to be enforced, including granting to state attorneys general the ability to respond to HIPAA privacy and security violations and to take appropriate action with respect to violators within their jurisdiction. Under the HITECH Act, state attorneys general may bring a civil action to enjoin violations of HIPAA and to seek damages for such violations. In effect, the HITECH Act has empowered state attorneys general to act, along with OCR, to enforce the HIPAA privacy and security rules.[3]

Furthermore, as an administrative matter, covered entities routinely enter into arrangements with third-party service providers to perform administrative functions requiring the use or disclosure of protected health information. Since the inception of the HIPAA privacy and security rules, such "business associates" of covered entities have had contractual obligations to abide by the same restrictions on the use and disclosure of protected health information that apply to covered entities. Changes under the HITECH Act have also introduced a brand new playing field for business associates. From now on, the business associates of covered entities are, much as covered entities have always been, directly subject to the civil and criminal penalties that may be imposed by OCR under HIPAA. As a result, business associates must take action to ensure that they have adopted policies and procedures applicable to the privacy and security of the protected health information that they use and disclose in the course of performing services for covered entities.

The Most Recent OCR Enforcement Actions

OCR has previously imposed sanctions under settlement agreements with cooperative covered entities for violations of HIPAA. In the first civil money penalty ever imposed by OCR, Cignet Health, of Prince George's County, Maryland was ordered in February to pay $4.35 million for HIPAA violations arising from the covered entity's failure to provide 41 patients with access to their protected health information (such access is required according to procedures and timeframes outlined in the privacy regulations) as well as the covered entity's failure to cooperate with OCR's investigation.[4] Indeed, by failing to cooperate more fully with OCR's investigation of the patients' complaints (itself a violation of HIPAA that is subject to sanction), Cignet Health acted with the kind of "willful neglect" that in the view of OCR made it liable for the most stringent monetary penalties. $3 million of the $4.35 million sanction was attributable to Cignet Health's failure to cooperate.[5]

In another sanction announced in February, OCR entered into a settlement agreement with General Hospital Corporation and Massachusetts General Physicians Organization, Inc. ("Mass General"). The settlement agreement provides for the payment of $1 million to resolve alleged multiple disclosure

violations that occurred when a Mass General employee misplaced on the subway paper medical records containing the protected health information of 192 patients.[6] It is worth noting that Mass General appears to have cooperated with the OCR investigation and worked with OCR to reach an agreement to resolve the violations at issue. Among other things, Mass General's settlement agreement with OCR included the creation of a corrective action plan to be temporarily monitored by OCR.

Why the First Ever Civil Penalty May Have Been Imposed Now, and Lessons Learned

While to some observers the penalties in both cases appear disproportionate to the violations at issue, it has to be emphasized that Mass General appears to have cooperated much more fully with the OCR investigation of its alleged HIPAA violations than did Cignet Health. By cooperating with OCR, Mass General almost certainly avoided even more stringent penalties that could have been imposed for the single action of one of its employees.

If nothing else, these cases are a pointed reminder that stricter enforcement of HIPAA is probably here to stay, and that it is imperative for covered entities and business associates to cooperate fully with OCR in the event of any investigation of an alleged violation. Covered entities and business associates must also take action to ensure that adequate policies and procedures are in place and up to date. For covered entities, this will mean consulting with specialists to review and revise as necessary existing policies and procedures for changes in the law under the HITECH Act. For business associates, this will probably mean establishing for the first time written policies to implement procedures for the protection of individually identifiable health information.

Furthermore, because of the civil and criminal monetary greater penalties that may now apply, it is more important than ever for covered entities and their business associates to make sure they have in place the required compliance safeguards and conduct the periodic workforce training in compliance that is required by the HIPAA privacy and security regulations. Training may include an emphasis on a common sense approach, such as a simple prohibition on the movement of protected health information outside of a secure workplace. Not only is such training a good practice to avoid potentially costly errors, it would serve as evidence in the event of an investigation by OCR of an awareness of and a commitment to ongoing compliance with HIPAA requirements. As the recent OCR enforcement actions demonstrate, that may go far in reducing the business risk of substantial losses for compliance failures. Only then may covered entities and business associates hope to avoid the increasingly significant monetary sanctions under HIPAA that are going to be the rule for the foreseeable future.

Andrew Elbon is a partner in the Employee Benefits and Executive Compensation group at Bradley Arant Boult Cummings LLP. His practice is focused on compliance issues relating to the design and administration of employee benefit plans, including the protection of health information under the privacy and security regulations imposed on group health plans by HIPAA.

---

[1] Copies of the final OCR determination and the settlement agreement in these cases may be found at http://www.hhs.gov/ocr

[2] As discussed below, the maximum dollar amount of these penalties has been significantly increased under recent legislation.

[3] Indeed, the Department of Health and Human Services recently announced that it would present enforcement training courses for state attorneys general.

[4] *See* http://www.hhs.gov/ocr/privacy/hipaa/news/cignetnews.html

[5] For more detail about the action against Cignet, see *HHS Imposes $4.3 Million Penalty for HIPAA Violations*, Bloomberg Law Reports - Privacy & Information, Vol. 4, No. 3 (March, 2011)

[6] *See* http://www.hhs.gov/ocr/privacy/hipaa/news/mghnews.html