The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently issued fines against two violators of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule – one in the form of a civil monetary penalty and one in the form of a settlement amount. In demanding payment for violations of the HIPAA Privacy Rule, HHS evidenced that it is serious about enforcing the HIPAA Privacy Rule and will take all necessary steps to ensure that covered entities are affording individuals the rights to which they are entitled under HIPAA.

Cignet Fined a $4.3 Million Civil Monetary Penalty for HIPAA Privacy Rule Violations

HHS issued a civil monetary penalty assessed against Cignet Health of Prince George’s County, Maryland (Cignet), based on its failure to provide patients with access to their medical records required by the HIPAA Privacy Rule ($1.3 million) and for Cignet’s failure to cooperate with OCR’s investigation ($3 million). The civil monetary penalty is significant both in its amount and because it is the first time HHS has assessed such a penalty against a covered entity for failure to comply with HIPAA.

After investigating certain patient complaints directed at Cignet, OCR determined that Cignet violated 41 patients’ rights under HIPAA by denying them access to their medical records when requested between September 2008 and October 2009. The HIPAA Privacy Rule requires that a covered entity, upon patient request, provide patients with a copy of their medical records within 30 (and no later than 60) days of the request. In addition, during OCR’s investigation of the patient complaints, Cignet refused to respond to OCR’s demands to produce records and made no efforts to resolve the patient complaints through informal means. OCR determined that by doing so, Cignet willfully neglected its obligation to cooperate with OCR’s investigation.
Mass General and HHS Settle Potential HIPAA Privacy Rule Violations for $1 Million

Just two days after HHS disclosed the civil monetary penalty assessed against Cignet, it announced that it had entered into a resolution agreement with the General Hospital Corporation and Massachusetts General Physicians Organization, Inc. (Mass General) pursuant to which Mass General agreed to pay $1 million dollars to settle potential violations of the HIPAA Privacy Rule.

The incident that gave rise to the resolution agreement involved the loss of protected health information of 192 patients of Mass General’s Infectious Disease Associates outpatient practice, including patients with HIV/AIDS. More specifically, a Mass General employee, while commuting to work, left documents on the subway train that included a patient schedule and medical record numbers for 192 patients, as well as billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis and name of providers for 66 of such patients.

The resolution agreement also requires Mass General to enter into a Corrective Action Plan (CAP) with HHS. Pursuant to the CAP, Mass General is required to develop and implement a comprehensive set of policies and procedures to safeguard the privacy of its patients, including policies that specifically address physical removal and transport of protected health information, laptop encryption, and USB-drive encryption. Mass General must provide training to its workforce on such policies and procedures. Further, Mass General is required to appoint a Director of Internal Audit Services to implement a monitoring plan that includes unannounced site visits, interviews of staff, and inspections of laptops and USB flash drives. The Director of Internal Audit Services must submit reports to OCR every six months, summarizing the results of the monitoring activities.

Impact for Covered Entities

In light of the recent privacy breaches and HHS’ enforcement actions, covered entities should be mindful of the following:

> **Review and Update HIPAA Policies.** Because the use of mobile devices by covered entities and their workforce members is on the rise, covered entities should adopt and implement policies and procedures that specifically address the use of such devices, as well as the removal of protected health information outside the entity (in paper or electronic form) and encryption of mobile devices.

> **Training on HIPAA Policies.** Covered entities should be sure members of their workforce read, understand and follow applicable HIPAA policies. The above may be accomplished through meaningful, regular training so that workforce members understand how the covered entity’s HIPAA policies apply to their day-to-day job duties.
> **Monitoring.** A key component of Mass General’s CAP is ongoing HIPAA compliance monitoring. A robust internal audit/monitoring program will help identify problems early and minimize risk. Improper uses or disclosures of protected health information should be addressed without delay and appropriate corrective action should be taken promptly.

> **Track New Developments.** The final regulations implementing certain provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act are expected to be published in the near future. Covered entities should stay abreast of new developments and take immediate action to implement updated policies and procedures that address applicable changes. Drinker Biddle’s Health Law Practice Group will issue additional client alerts as applicable when the HITECH Act Final Rule is published.

---

**Drinker Biddle Welcomes Noted Privacy Lawyer**

Drinker Biddle welcomes Stan Crosley as Of Counsel to the firm. Stan is the Co-Director of the Indiana University Center for Strategic Health Information Provisioning, a health information strategy and management center created through IU’s schools of Law, Medicine and Informatics. He is also the former Chief Privacy Officer for Eli Lilly Company, where he initiated Lilly’s global privacy program in 1998. The program received the 2007 Innovation Award from the International Association of Privacy Professionals. Stan also co-founded and served as Chair of the International Pharmaceutical Privacy Consortium and was a member of the IOM Medical Research and Privacy Committee. He serves on the boards of the Indiana Health Informatics Technology, Inc., the International Association Privacy Professionals, and The Privacy Projects and is a member of the Brookings Institute Experts’ Committee on Active Medical Product Surveillance.

Stan will join Drinker Biddle’s existing privacy practitioners as leader of its cross-disciplinary Data Privacy & Health Information Governance Team.