DrinkerBiddle

Client Alert

February 22, 2017

Costly Failure to Safeguard Protected Health Information from Unauthorized Staff

By Katherine E. Armstrong, Jennifer R. Breuer and Sumaya M. Noush

Key Takeaways

- $5.5 million payment– tied for the highest HIPAA settlement amount
- Important to review audit reports and trails for suspicious activity and maintain access controls

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) has kept up its rapid and aggressive enforcement of the Health Insurance Portability and Accountability Act (HIPAA) with another sizeable settlement. South Broward Hospital District, operating as Memorial Healthcare Systems (MHS), paid OCR $5.5 million to settle potential violations of HIPAA and agreed to a three-year corrective action plan. MHS is the third largest public health care system in the nation and it holds the spot for the third OCR HIPAA settlement and fourth HIPAA action of 2017.

On April 12, 2012, MHS reported to HHS that two of its employees inappropriately accessed protected health information (PHI), including patient names, dates of birth, and social security numbers. After an internal investigation, MHS discovered impermissible access by 12 users at affiliated physician offices that potentially affected another 105,646 individuals. According to the resolution agreement, some of the instances of impermissible access led to federal charges relating to the selling of protected health information and filing fraudulent tax returns.

Despite MHS having identified the risk on several occasions before the privacy breach occurred, OCR's investigation revealed that MHS impermissibly provided access to PHI to a former employee of an affiliated physician's office which resulted in the impermissible disclosure of PHI of 80,000 individuals. In addition to this violation of the HIPAA Privacy Rule, OCR also determined that MHS failed to implement procedures to regularly review records of information system activity and failed to implement policies and procedures that establish, document, review and modify a user's right of access to electronic PHI (ePHI) as required by the HIPAA Rules.

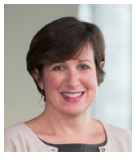
This large breach and settlement serves as a reminder of the importance for covered entities and business associates to use and review audit logs and audit trails that provide information on which users are accessing what types of PHI in order to stop suspicious system activities.

If you have any questions about this settlement or HIPAA compliance, please contact any member of Drinker Biddle's Health Care Team or Information Privacy, Security and Governance Team.

Information Privacy, Security and Governance Team

Primary Contacts

Katherine E. Armstrong
Counsel
Washington
(202) 230-5674
Katherine.Armstrong@dbr.com



Jennifer R. Breuer
Partner
Chicago
(312) 569-1256
Jennifer.Breuer@dbr.com

Sumaya M. Noush
Associate
Chicago
(312) 569-1268
Sumaya.Noush@dbr.com