Drinker Biddle

Client Alert

April 17, 2017

A Failure to Plan is a Plan to Fail: $400,000 OCR Settlement Highlights the Importance of Risk Assessments and Management Plans

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

Key Takeaway:

- HIPAA requires Covered Entities to proactively conduct risk assessments and implement risk management plans to prevent data breaches

Metro Community Provider Network (MCPN) has entered into a $400,000 Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement and three-year corrective action plan with the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR). The parties settled MCPN's potential noncompliance with the HIPAA Privacy and Security Rules, stemming from a phishing incident that gave impermissible access to the electronic protected health information (ePHI) of 3,200 individuals.

MCPN – a federally qualified health center located in Colorado that serves approximately 43,000 low-income patients annually – filed a HIPAA Breach Notification Report on January 27, 2012, following the phishing incident. Although OCR determined that MCPN took necessary corrective action related to the phishing incident itself, MCPN had failed to conduct any prior risk assessments to detect the vulnerabilities in its ePHI environment as required by HIPAA. More specifically, OCR's investigation revealed that MCPN failed to (1) implement policies and procedures to prevent, detect, contain, and correct security violations, and (2) failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

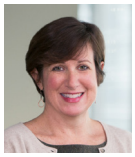
Per its corrective action plan, MCPN must conduct a risk analysis and implement a risk management plan to reduce or eliminate any risks to ePHI. MCPN must also review and revise its current Security Rule Policies and Procedures based on its findings and the implementation of its risk management plan. Lastly, MCPN is required to update its current Security Rule training materials to reflect the new information it gathers regarding its risks and any of the revisions MCPN makes to its policies and procedures. HHS will review the training materials and ultimately require MCPN to administer a Security Rule training program to each member of its workforce who has or will have access to ePHI.

This OCR HIPAA settlement, reached less than one month after Roger Severino's appointment as OCR Director in late March 2017, indicates that there is no slowing down on HIPAA enforcement at HHS under the new administration. Recent HIPAA settlements such as this one emphasize the importance of properly conducting risk analyses and implementing risk management plans to secure ePHI. The OCR's press release on the settlement is available here.

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.

Health Care Industry Team

Primary Contacts



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

Katherine E. Armstrong
Counsel
Washington, D.C.
(202) 230-5674
katherine.armstrong@dbr.com

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

Drinker Biddle®

www.drinkerbiddle.com

CALIFORNIA | DELAWARE | ILLINOIS | NEW JERSEY | NEW YORK | PENNSYLVANIA | TEXAS | WASHINGTON DC | LONDON