Tips for Ensuring Your Organization Is HIPAA Compliant Amid Increased Enforcement Activity

Thus far in 2017, the U.S. Department of Health and Human Service's Office for Civil Rights has continued the step-up in HIPAA enforcement activity we saw in 2016 and appears on track to exceed 2016's enforcement activity.

From January through early May, OCR already has published settlements with eight different health care entities—ranging from small providers to large health systems—for HIPAA violations and levied penalties totaling nearly $17 million.

By comparison, in 2016, OCR announced settlements with 12 health care entities and levied penalties of approximately $23 million. The 2017 settlements thus far include:

- $475,000 against Illinois health system Presence Health in the first enforcement action for failure to notify affected individuals and prominent media outlets of a breach within the 60-day deadline set by HIPAA;
- $2.2 million against MAPFRE Life Insurance Company of Puerto Rico arising from the theft of a USB storage data device left overnight in its IT department, its failure to conduct a risk analysis and implement risk management plans, and its failure to encrypt laptops or removable storage media prior to 2014;
- $3.2 million against Children's Medical Center of Dallas arising from the loss of an unencrypted, non-password-protected Blackberry and Children's failure to implement risk management plans or encrypt mobile devices until 2013 despite apparently being aware since 2007 of the risks of storing unencrypted ePHI on its devices;
- $5.5 million against Florida health system Memorial Healthcare System arising from impermissible access and disclosure of ePHI to affiliated physician office staff using the login credentials of a former employee whose credentials were not terminated in accordance with workforce access policies and were used on a daily basis without detection for a year;
- $400,000 against Metro Community Provider Network, a federally qualified health center in Denver, relating to OCR's discovery that MCPN had never conducted a risk analysis or implemented a risk management plan prior to a phishing incident in 2012;
- $31,000 against a small Illinois provider, Center for Children's Digestive Health, for the failure to have a Business Associate Agreement with one vendor;
- $2.5 million against wireless device manufacturer CardioNet arising from the theft of a workforce member's laptop and the fact that CardioNet's policies and procedures implementing the HIPAA Security Rule standards were in draft form and had never been implemented; and
- $2.4 million against Texas health system Memorial Hermann Health System arising from the issuance, approved by senior management, of a press release to several media outlets disclosing the PHI of a patient who was arrested after presenting an allegedly fraudulent identification card to office staff.

When OCR imposes civil monetary penalties, it memorializes them in a Resolution Agreement and Corrective Action Plan. The Resolution Agreement generally permits a health care entity to avoid admitting liability for the HIPAA breach, provided that it enters into a Corrective Action Plan detailing the steps the health care entity will be

required to make to remedy the breach. The Corrective Action Plan is typically in place for two or three years unless the health care entity breaches the CAP, in which case it may be extended.

CAP requirements can be extensive and burdensome and often require the health care entity to:

- Revise, and submit to OCR for review and approval, certain HIPAA-required policies and procedures (including risk assessments, risk management plans, and training programs);
- Retrain all workforce members who have access to PHI on HIPAA compliance;
- Provide to OCR certain information such as a certification that all devices have been encrypted or copies of all the health care entity's business associate agreements;
- Develop, and submit to OCR for review and approval, a plan for an internal or external monitor to review the health care entity's compliance with the CAP; and
- Submit detailed annual reports to OCR describing compliance efforts required by the CAP.

The takeaway to Covered Entities and Business Associates from these recent enforcement actions is that now is the time to get your HIPAA compliance efforts in order. Your organization's privacy officer can start by taking the following actions:

- Review and, if necessary, update HIPAA risk assessments and risk management plans;
- Ensure that all required HIPAA policies and procedures have been finalized and formally approved by your organization;
- Review whether your organization's HIPAA policies and procedures are being followed in practice because, as the Memorial Healthcare System settlement demonstrates, OCR will not look favorably upon an organization that fails to follow its own policies and procedures;
- Review breach response procedures and ensure that a breach response team is in place to quickly assess a potential breach and, if necessary, ensure that notifications are issued within the 60-day deadline;
- Ensure that all necessary Business Associate Agreements are in place;
- Ensure that your organization's communications policy incorporates HIPAA; and
- Determine whether your organization has or needs an insurance policy covering HIPAA breaches.

If you would like help ensuring your organization is fully HIPAA-compliant, please contact **Brownstein** for assistance.

Erin M. Eiselein
Shareholder
eeiselein@bhfs.com
303.223.1251

Anna-Liisa Mullis
Associate
amullis@bhfs.com
303.223.1165