HIPAA Privacy & Security Updates

From Dorothy Cociu, COIN Editor and HIPAA Privacy & Security Consultant & Trainer

May/June, 2017

As an update on HHS/OCR enforcement actions, a few important settlements were reported in April, 2017.

On April 12, 2017, HHS/OCR announced a HIPAA settlement based on the lack of a security management process to safeguard electronic PHI (ePHI). Metro Community Provider Network (MCPN), a federally-qualified health center, agreed to settle potential non-compliance with the HIPAA Privacy & Security Rules by paying $400,000 and implementing a corrective action plan. On January 27, 2012, MCPN filed a breach report with OCR indicating that a hacker accessed employees' email accounts and obtained 3,200 individuals' ePHI through phishing incident. OCR's investigation revealed that MCPN failed to conduct a risk analysis until mid-February, 2012 (after the incident). The investigation also revealed that MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in it's ePHI environment, and consequently, had not implemented any corresponding risk management plans to address risks and vulnerabilities identified in a risk analysis. When finally conducted, that analysis, as well as all subsequent risk analyses, were insufficient to meet the requirements of the Security Rule.

On April 20, 2017, HHS/OCR released a settlement action for The Center for Children's Digestive Health (CCDH), which reported that they had paid a sum of $31,000 and agreed to implement a corrective action plan, for failure to have a Business Associates Agreement in place. CCDH is a small, for-profit health care provider with a pediatric subspecialty practice that operates in seven clinic locations in Illinois.

On April 24, 2017, HHS/OCR announced a $2.5 million settlement which shows that not understanding HIPAA requirements creates a risk. CardioNet agreed to a settlement based on the impermissible disclosure of unsecured ePHI. They must also implement a corrective action plan. CardioNet provides remote mobile monitoring of and rapid response to patients at risk for cardiac arrhythmias.

In January, 2012, CardioNet reported to HHS/OCR that a member's laptop was stolen from a parked vehicle outside of the employee's home. The laptop contained the ePHI of 1,391 individuals. OCR's investigation into the impermissible disclosure revealed that CardioNet had an insufficient risk analysis and risk management process in place at the time of the theft. Additionally, CardioNet's policies and procedures implementing the standards of the HIPAA Security Rule were in draft form and had not been implemented. Further, the Pennsylvania-based organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

##