Overlooking risks leads to breach, $400,000 settlement, April 12, 2017

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

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR), has announced a Health Insurance Portability and Accountability Act of 1996 (HIPAA) settlement based on the lack of a security management process to safeguard electronic protected health information (ePHI). Metro Community Provider Network (MCPN), a federally-qualified health center (FQHC), has agreed to settle potential noncompliance with the HIPAA Privacy and Security Rules by paying $400,000 and implementing a corrective action plan. With this settlement amount, OCR considered MCPN's status as a FQHC when balancing the significance of the violation with MCPN's ability to maintain sufficient financial standing to ensure the provision of ongoing patient care. MCPN provides primary medical care, dental care, pharmacies, social work, and behavioral health care services throughout the greater Denver, Colorado metropolitan area to approximately 43,000 patients per year, a large majority of whom have incomes at or below the poverty level.

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 a phishing incident. OCR's investigation revealed that MCPN took necessary corrective action related to the phishing incident; however, the investigation also revealed that MCPN failed to conduct a risk analysis until mid-February 2012. Prior to the breach incident, MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment, and, consequently, had not implemented any corresponding risk management plans to address the risks and vulnerabilities identified in a risk analysis. When MCPN finally conducted a risk analysis, that risk analysis, as well as all subsequent risk analyses, were insufficient to meet the requirements of the Security Rule.

The Resolution Agreement and Corrective Action Plan may be found on the OCR website at http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/MCPN