2012 Issue 6

www.ober.com

SPECIAL FOCUS: HIPAA/PRIVACY

OCR Settles with Small Physician Practice for HIPAA Violations

By: Sarah E. Swank

On the heels of its $1.5 million settlement with a large payor, Blue Cross Blue Shield of Tennessee, the Department of Health and Human Services Office for Civil rights (OCR) announced on April 17, 2012, that it settled with a small physician practice for HIPAA violations. Phoenix Cardiac Surgery, P.C., a practice owned by two physicians, entered into a settlement agreement [PDF] and agreed to pay $100,000 after OCR found the practice lacked adequate HIPAA safeguards.

Over a year-and-a-half period, the practice posted 1,000 entries of ePHI on a publically accessible, Internet-based calendar. In addition, over three years the practice transmitted ePHI on a daily basis over an Internet-based email account to workforce members' personal Internet- based email accounts. OCR, after investigation of a complaint, found that the physician practice failed to:

- Implement adequate policies and procedures to appropriately safeguard patient information
- Document that it trained any employees on its policies and procedures on the HIPAA Privacy Rule and Security Rule
- Identify a security officer and conduct a risk analysis
- Obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of it ePHI and access to its ePHI

Along with the $100,000 payment to OCR, the practice also agreed to enter into a corrective action plan (CAP) requiring that it develop, maintain and revise written HIPAA policies and procedures and submit them to OCR for approval prior to

implementation. Within 30 days of OCR approval, the practice must implement these policies and procedures and distribute them to its workforce members. Within 60 days of OCR approval, the practice must provide training to all workforce members. The CAP also requires that the practice assess, review and revise its HIPAA polices and procedures at least annually or more frequently, as appropriate. Should any additional violations occur related to its HIPAA polices and procedures, the practice must submit a report directly to OCR within 30 days from its determination of a violation, including: a description of the events, persons involved, actions taken to mitigate any harm and any further steps the practice plans to take to address the matter and prevent the violations from happening again.

In a press announcement, Leon Rodriguez, Director of OCR emphasized, "We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity." Small physician practices should take note that they are not immune to OCR investigation.