Arnall Golden Gregory LLP

Client Alert

Contact Attorney Regarding This Matter:

Sidney S. Welch
404.873.8182 – direct
sidney.welch@agg.com

Arnall Golden Gregory LLP
Attorneys at Law

171 17th Street NW
Suite 2100
Atlanta, GA 30363-1031

One Biscayne Tower
Suite 2690
2 South Biscayne Boulevard
Miami, FL 33131

2001 Pennsylvania Avenue NW
Suite 250
Washington DC 20006

www.agg.com

Small Physician Practice Pays $100,000 to Settle HIPAA Violations

Recently, the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced in a press release that it has entered into a Resolution Agreement that requires Phoenix Cardiac Surgery PC, a small cardiology practice based in Phoenix and Prescott, Arizona, to pay $100,000 to HHS and implement a Corrective Action Plan. The settlement with the physician practice follows an extensive investigation by OCR for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

According to the press release, the incident that gave rise to OCR's investigation was a report that the physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was accessible to the public. As part of its investigation, OCR concluded that the physician practice had implemented few policies and procedures to comply with HIPAA, and had limited safeguards in place to protect patients' electronic protected health information (ePHI). OCR identified the following issues during its investigation:

1. The practice failed to implement adequate policies and procedures to appropriately safeguard patient information;

2. The practice failed to document that it trained any employees on its policies and procedures on the Privacy and Security Rules;

3. The practice failed to identify a security official and conduct a risk analysis; and

4. The practice failed to obtain business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.

As part of the Corrective Action Plan, the physician practice agreed to develop a comprehensive set of HIPAA policies and procedures and to submit them to OCR for review and approval. After OCR has approved the policies and procedures, the practice is required to implement them and train all members of its workforce who use or disclose protected health information on their requirements. Additionally, the Corrective Action Plan states that the policies and procedures must include the following specific content:

1. A thorough assessment of the risks and vulnerabilities to ePHI;

2. A risk management plan to reduce any risks and vulnerabilities identified by the risk assessment;

3. The identification of a HIPAA Security Official;

4. Satisfactory assurances that each business associate will safeguard ePHI pursuant to a contract that contains the HIPAA Privacy and Security Rule provisions required in business associate agreements;

5. Technical safeguards that restrict access to ePHI;

6. Technical measures to protect ePHI transmitted over an electronic communications network, including via text messaging; and

7. Training, including security reminders and procedures for guarding against malicious software.

This settlement serves as an important reminder to physician practices to review compliance with the HIPAA Privacy and Security Rules.