



## Client Alert

Contact Attorneys Regarding  
This Matter:

Aaron M. Danzig  
404.873.8504 – direct  
[aaron.danzig@agg.com](mailto:aaron.danzig@agg.com)

Erin R. Kendall  
404.873.7030 – direct  
[erin.kendall@agg.com](mailto:erin.kendall@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](http://www.agg.com)

### HHS Settles With Small Medical Practice For HIPAA Violations

Phoenix Cardiac Surgery, P.C., a five doctor medical practice based in Phoenix, Arizona, entered into a settlement agreement with the U.S. Department of Health and Human Services (“HHS”) to pay \$100,000 and take corrective actions for violating the Health Insurance Portability and Accountability Privacy Act (“HIPAA”). Phoenix Cardiac Surgery, P.C. is the first small medical practice to be charged with violating HIPAA’s Privacy and Security Rules. This settlement agreement is a warning to doctors that, no matter the size of your practice, you can be held accountable for HIPAA violations.

The HHS Office for Civil Rights (“OCR”) launched an investigation into Phoenix Cardiac Surgery, P.C. after a complaint was filed alleging that the practice was posting surgery and appointment schedules on an Internet-based calendar that was accessible to the public. As the investigation progressed, it became clear that the medical practice had done little to comply with HIPAA Privacy and Security Rules since the regulations were implemented. OCR’s investigation revealed the following issues:

- The medical practice failed to implement adequate policies and procedures to appropriately safeguard patient information;
- The medical practice failed to document that it trained any employees on its policies and procedures on the Privacy and Security Rules;
- The medical practice failed to identify a security official and conduct a risk analysis; and
- The medical 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.

Leon Rodriguez, director of OCR, stated that “[t]his case is significant because it highlights a multiyear, continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules,” and “[w]e 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.”

The HHS Resolution Agreement with Phoenix Cardiac Surgery, P.C. can be found [here](#).

*Arnall Golden Gregory LLP serves the business needs of growing public and private companies, helping clients turn legal challenges into business opportunities. We don't just tell you if something is possible, we show you how to make it happen. Please visit our website for more information, [www.agg.com](http://www.agg.com).*

*This alert provides a general summary of recent legal developments. It is not intended to be, and should not be relied upon as, legal advice.*