Two-Owner Physician Practice Pays $100,000 to Settle Claims of HIPAA Violations

June 11, 2012

A recent case indicates that the government is looking into HIPAA violations by small medical practices as well as large institutional providers, and the results can be expensive.

Following an investigation by the United States Department of Health and Human Services (HHS) Office for Civil Rights (OCR) into potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HHS recently entered into a $100,000 settlement with Phoenix Cardiac Surgery, P.C. (Phoenix) that required Phoenix to take corrective action to implement policies and procedures to safeguard protected health information of its patients. Phoenix is a two-owner medical practice.

The OCR initiated its investigation of Phoenix based on a report that Phoenix was posting clinical and surgical appointments for patients on a public calendar on the Internet. Such information is considered electronic protected health information under HIPAA. The investigation showed that Phoenix had not implemented adequate policies and procedures to comply with the HIPAA Privacy and Security Rules, based on the following findings:

- Phoenix failed to train employees on policies and procedures regarding the Privacy and Security Rules, and failed to document such training.
- Phoenix failed to appoint a security official and conduct a risk assessment, as required by the Security Rule.
- Phoenix failed to implement adequate policies and procedures to appropriately safeguard patient information.
- Phoenix failed to obtain business associate agreements with Internet-based email and calendar service providers where the provision of the service included storage of and access to its electronic protected health information. It is important to note that the business associate agreement was required not only because of the Internet appointment postings, but also because Phoenix transmitted electronic protected health information from an Internet-based email account to employees personal Internet-based email accounts.

The settlement agreement required Phoenix to pay $100,000 and enter into a corrective action plan to ensure compliance with the HIPAA Privacy and Security Rules. This settlement highlights the fact that the OCR will investigate even small medical practices for HIPAA violations and that all practices must be aware of their obligations under the HIPAA Privacy and Security Rules.

If you would like more information about the information discussed in this Alert, please contact a member of the Health Care Practice Group at Flaster Greenberg P.C.

ATTORNEYS MENTIONED

Stephen Greenberg