HIPAA ENFORCEMENT -
NO PHYSICIAN OFFICE TOO SMALL

Tiny Cardiology Practice to Pay $100,000

Once again, the Office of Civil Rights (“OCR”) has bared its teeth and shown that no practice group is too small for enforcement action. Phoenix Cardiac Surgery, P.C. (“PCS”) learned the hard way on April 17, 2012, when OCR announced a settlement and Corrective Action Plan (the “Plan”) against the two-physician practice. To date, almost all OCR enforcement actions have been against large insurers and major hospital systems, not community hospitals or small physician practice groups. The settlement was unusual in many ways.

The nature of the alleged violation was a systemic, multi-year failure to adopt and implement appropriate HIPAA safeguards. The settlement amount of $100,000 was miniscule. The violation has yet to appear on OCR’s “Wall of Shame,” indicating that there is a possibility that the breach involved fewer than 500 individuals.

OCR’s investigation of PCS followed a report that PCS was posting surgical and clinical appointments for its patients on a publicly accessible Internet-based calendar. OCR also discovered the following issues:

- PCS failed to implement adequate policies and procedures to appropriately safeguard patient information;
- PCS failed to provide and document training of its employees on its policies and procedures relative to the HIPAA Privacy and Security Rules;
- PCS transmitted ePHI daily from an Internet-based email account to workforce members’ personal Internet-based email accounts;
- PCS failed to name a security officer and to conduct a risk analysis; and
- PCS failed to obtain business associate agreements with Internet-based email and calendar providers who stored and offered access to its ePHI.

This government enforcement action is clearly intended to send a stern reminder to small physician practices. It appears that OCR picked this practice at random simply because it was tiny and in clear violation of the HIPAA requirements. The Plan requires PCS to develop, maintain and revise, as necessary, written policies and procedures that are approved by OCR to meet the requirements of the HIPAA Privacy and Security Rules. All workforce members must receive these within 15 days of beginning employment, and PCS must obtain certification that employees have read, understand and will abide by such policies and procedures. PCS must update its risk assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI when it is created, received, maintained, used or transmitted by
PCS. This assessment must include ePHI: (a) posted to an Internet-based electronic calendaring system; (b) transmitted over an Internet-based electronic communications system; (c) accessed remotely; or (d) transmitted to or from or stored on a portable device. The Plan also requires numerous operational changes by PCS, including the requirement that PCS must report any violation of the policies and procedures by any member of the workforce to OCR within 30 days.

No Surprises - Practice was Nailed for Failure to Follow Basic Rules

OCR is requiring PCS to do what it should have been doing all along in order to meet the requirements of HIPAA. By going after this small physician practice, OCR is sending a message that no covered entity is too small to be penalized, and any compliance failure, no matter how few patients are affected, may receive the government’s baleful attention. All covered entities, regardless of how many employees or patients they have, need to be aware that OCR is prepared to strike at any time.

This OCR action follows closely on the heels of a $1.5 Million fine paid in March by Blue Cross Blue Shield of Tennessee. The fine stems from an incident in 2009, when an intruder illegally accessed a Blue Cross building and took more than fifty computer hard drives containing unencrypted information on about 1 million Blue Cross members. According to published reports, the recent fine brought Blue Cross Blue Shield’s total estimated costs related to this one breach to over $18 million.

In its press release, OCR noted:

“... BCBST failed to implement appropriate administrative safeguards to adequately protect information remaining at the leased facility by not performing the required security evaluation in response to operational changes. In addition, the investigation showed a failure to implement appropriate physical safeguards by not having adequate facility access controls; both of these safeguards are required by the HIPAA Security Rule.”

HIPAA enforcement is ramping up. If you have questions concerning HIPAA compliance, you should speak to your health care counsel or call:

Elizabeth Neuwirth, 203.772.7742, eneuwirth@murthalaw.com
Christina Hage, 203.772.7704, chage@murthalaw.com
Heather O. Berchem, 203.772.7728, hberchem@murthalaw.com
Kennedy Hudner, 860.240.6029, khudner@murthalaw.com
Paul E. Knag, 203.653.5407, pknag@murthalaw.com