Two Health Care Organizations Pay Largest HIPAA Fine at $4.8 Million Resulting from Unsecured Shared Network

New York-Presbyterian Hospital and Columbia University entered into a settlement with the Department of Health and Human Services' Office of Civil Rights (OCR) to resolve allegations that the organizations had violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) by failing to secure thousands of patients' electronic protected health information (ePHI) housed on the hospital and university's shared network. At $4.8 million—$3.3 million to be paid by New York-Presbyterian, and $1.5 million to be paid by Columbia University—this represents the largest HIPAA settlement to date. A fine of this magnitude for a technical security standard violation underscores OCR's commitment to impose harsh consequences to parties obligated to comply with HIPAA who fail to do so.

The alleged breach, which was reported jointly to the OCR by the organizations and occurred in September 2010, involved the unauthorized disclosure of the ePHI of 6,800 individuals, including their respective patient status, vital signs, medications, and lab results. The organizations reported the alleged breach promptly upon learning from an individual who had found a deceased partner's ePHI from New York-Presbyterian Hospital on the Internet. The investigation revealed that the breach was caused by a physician employed by Columbia University who created applications for both organizations had deactivated a personally owned computer server on the hospitals' shared network containing New-York Presbyterian patient information, which inadvertently resulted in patient information being accessible on Internet search engines.

OCR determined that the organizations lacked appropriate technical safeguards that would have prevented this breach, had failed to conduct accurate and thorough risk analyses on their systems that would have identified this vulnerability, and had failed to develop adequate risk management plans to address potential security threats to patient information. Finally, OCR determined that New York-Presbyterian also failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its policies on access management. Both parties agreed to prepare substantial corrective action plans to address their respective HIPAA program deficiencies.

Prior to this settlement, the largest HIPAA civil monetary penalty levied was for $4.3 million in 2011 against Cignet Health, Temple Hills, Md., a company that operates a health plan and four physician offices. Notably, however, $3 million of that fine was due to Cignet Health's failure to cooperate with the OCR's investigation into the allegations that Cignet Health had denied 41 patients access to their medical records in violation of their rights under HIPAA.

In the New York-Presbyterian Hospital and Columbia University settlement, no allegations of obstruction or failure to cooperate were lodged against the organizations, and the OCR noted that the organizations promptly and appropriately self-reported the breach upon discovery, notified the affected patients, and notified media outlets, as required by HIPAA for a breach of this magnitude.

This settlement demonstrates that OCR is upping the ante for HIPAA violations that could have been prevented by appropriate physical, technical and/or administrative safeguards. Accordingly, now is the time for covered entities and business associates alike to reevaluate their HIPAA programs to ensure compliance with both the Privacy and Security Standards of HIPAA.

410 17th Street, Suite 2200
Denver, Colorado 80202

May 8, 2014

This document is intended to provide you with general information regarding HIPAA settlements. The contents of this document are not intended to provide specific legal advice. If you have any questions about the contents of this document or if you need legal advice as to an issue, please contact the attorneys listed or your regular Brownstein Hyatt Farber Schreck, LLP attorney. This communication may be considered advertising in some jurisdictions.

Julie A. Sullivan
Associate
jsullivan@bhfs.com
T 303.223.1231

Darryl T. Landahl
Shareholder
dlandahl@bhfs.com
T 303.223.1117