NEWS

OCR Announces $1.7 Million HIPAA Settlement with Health Plan for Passive Breach of Online ePHI

07.15.2013

BY: BRIAN C. VICK

In its latest high-profile enforcement action, the Office of Civil Rights ("OCR") of the U.S. Department of Health and Human Services ("HHS") announced on July 11, 2013 that it had entered a $1.7 million settlement with a large private health plan for failing to properly secure ePHI stored in a web-based application database. The Resolution Agreement released by OCR indicated that the health plan's management of the database failed to comply with the HIPAA Security Rule, and, as a result, unsecured ePHI of 612,402 individuals was left accessible over the internet for almost five months. Specifically, OCR identified compliance issues related to the adequacy of:

- the policies and procedures that governed access to ePHI stored in the application database;
- the technical evaluation of software upgrades to the database; and
- the technological measures implemented to verify the identity of individuals accessing ePHI stored in the database.

Notably, OCR's announcement did not give any indication that any unauthorized access had actually occurred. Unlike the settlements in other recent high-profile HIPAA enforcement actions, OCR did not incorporate a corrective action plan in the Resolution Agreement with the health plan and, instead, simply imposed a monetary penalty.

This settlement serves as another reminder that any entity that stores, maintains, transmits, or otherwise handles ePHI must pay close attention to its HIPAA obligations when managing the technical aspects of its information systems. Whenever implementing, upgrading, or reconfiguring a system that contains ePHI, entities should perform a HIPAA risk assessment to ensure that such changes do not adversely affect the security and accessibility of that ePHI. Robust and open communication between security officials and IT staff is critical to this process and should be something to which all HIPAA-covered entities pay close attention.

OCR's announcement of this settlement also highlights the need for HIPAA-covered entities to take steps to ensure that – by September 23, 2013 – they are in compliance with the new HIPAA rules governing business associates and subcontractors. Although OCR did not give any indication that a business associate was responsible for or involved in the health plan's breach, OCR used the accompanying press release to reiterate the deadline on which certain substantive requirements of

HIPAA will apply directly to business associates. Based on this announcement and comments made by OCR officials during recent presentations, business associate compliance is clearly an issue of high-priority for the agency and, if the past is any guide, will likely be a central feature of an OCR enforcement action in the near future.

For more information about this topic, you may contact the author or any member of the Williams Mullen eDiscovery and Information Governance Team or the Williams Mullen Health Care Team.

Related People

Related Services

- Health Care
- eDiscovery and Information Governance
- Litigation