Recent HIPAA settlement reinforces importance of encryption, risk analysis, and mobile device security

Richard H. Blake, James J. Giszczak, Rick L. Hindmand, Dominic A. Paluzzi | Wednesday, September 9, 2015

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently announced its settlement with an Indiana radiation oncology group under the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules for failure to conduct an enterprise-wide risk analysis and adopt written policies on the removal of electronic media. Cancer Care Group, P.C. (CCG), a 13-physician group practice, agreed to pay $750,000 and implement a robust corrective action plan.

Background

OCR initiated an investigation after CCG submitted a breach report on the 2012 theft of a laptop bag from an employee's car. Although the laptop did not contain electronic protected health information (ePHI), the bag also included unencrypted computer server backup media with ePHI on approximately 55,000 current and former CCG patients. OCR found widespread noncompliance with the Security Rule, including CCG's failure to conduct an enterprise-wide risk analysis and the lack of any written policy on the receipt and removal of hardware and electronic media containing ePHI. These shortcomings were particularly significant in light of OCR's determination that a risk analysis could have revealed the risks from removing unencrypted backup media from CCG's facility and that a comprehensive device and media control policy could have provided direction to employees.

Recent HIPAA settlement reinforces importance of encryption, risk analysis, and mobile device security

The settlement, which was dated Aug. 31 and announced Sept. 2, reinforces a long line of OCR enforcement actions and resolution agreements focusing on risk analysis of security risks and vulnerabilities, and also highlights the challenges with mobile device security. The press release includes the following warning from OCR Director Jocelyn Samuels:

> *Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information. Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information.*

OCR conference

In addition, risk analysis, encryption and mobile device security were recurring themes at an OCR cosponsored conference last week (Sept. 2 and 3, 2015) on Safeguarding Health Information. OCR Director Jocelyn Samuels, as well as other speakers from OCR, the Federal Trade Commission (FTC), and other agencies, described risk analysis and risk management as cornerstones to security. Covered entities and business associates will face additional scrutiny with OCR's HIPAA audits, which OCR officials assured last week will begin soon.

At last week's conference, Iliana Peters, the senior advisor for compliance and enforcement at OCR, praised CCG for providing innovative radiation oncology services to patients who otherwise wouldn't have access. This wasn't enough, however, to prevent OCR from pursuing CCG for HIPAA violations. The CCG settlement provides an important reminder that doing good doesn't excuse even an innovative physician practice from its obligations to safeguard patient information.

Takeaways

Covered entities and business associates should learn from this HIPAA settlement (and the other similar recent ones). It is essential to conduct ongoing risk analyses and implement encryption for ePHI both at rest and in motion. When the inevitable happens, make certain that you have an Incident Response Team and Incident Response Plan in place to respond to any potential compromise of PHI. The resulting regulatory investigations and enforcement actions are more frequent and complex than ever before. Make sure your organization is implementing the necessary proactive measures now, while things are calm. You don't want to be the next one writing a big check to HHS OCR.

OCR's press release is available on the U.S. Department of Health & Human Services' **website** along with the resolution agreement.

For more information, please contact one of the attorneys listed below.

Richard H. Blake

James J. Giszczak

Recent HIPAA settlement reinforces importance of encryption, risk analysis, and mobile device security

Rick L. Hindmand

Dominic A. Paluzzi