The New Normal: OCR's Newest HIPAA Settlement is Largest Ever

08.24.2016

What happens when a health care provider experiences several breaches, affecting a staggering 4 million people? Advocate Health Care Network (?Advocate?), an Illinois health system, found out the **hard way** after a subsidiary reported to the Department of Health and Human Services (?HHS?) three breaches of electronic protected health information in 2013. The breaches resulted from (1) a theft of four desktop computers, (2) unauthorized access to a business associate?s computer network, and (3) the theft of an unencrypted laptop from an unlocked vehicle. After a roughly three-year investigation, HHS? Office for Civil Rights (?OCR?) settled with Advocate for $5.55 million, the largest settlement by a single entity to date for a HIPAA violation.

OCR identified multiple ways in which Advocate failed to comply with the Security Rule requirements for protecting ePHI:

- Failure to perform an adequate risk analysis;
- Failure to implement physical safeguards and related policies and procedures;
- Failure to safeguard the ePHI of the individuals affected by the desktop computer and laptop breaches; and
- Failure to have a business associate agreement with its billing company, resulting in impermissible disclosures.

As a part of the **Corrective Action Plan** (?CAP?), Advocate, with OCR?s involvement and oversight, is required to:

- Develop and/or modify its risk analysis, risk management plan, and multiple categories of policies and procedures;
- Create a process ?to regularly evaluate any environmental and operational changes that affect the security of ePHI in Advocate?s possession or control including Advocate?s acquisition of new entities?;

- Develop internal monitoring and security training programs; and
- Report to OCR on its level of encryption for all electronic media.

In order to evaluate Advocate?s compliance with the CAP, OCR is requiring Advocate to hire an independent assessor and submit status updates to OCR, including specific documentation of compliance.

In addition to the large number of individuals affected by Advocate?s breaches, OCR noted additional factors that informed its valuation of the potential fine and ultimately its settlement. Such factors include a long period of noncompliance as well as the involvement of the Illinois Attorney General, who conducted an independent investigation and provided support and information to OCR.

OCR Director Jocelyn Samuels stated that ?We hope this settlement sends a strong message to covered entities that they must engage in a comprehensive risk analysis and risk management to ensure that individuals? ePHI is secure.? OCR has been quite clear that conducting a thorough, entity-wide risk analysis (and making substantive changes based on the identified risks) has been and will continue to be a key focus of OCR?s compliance and enforcement efforts. Now that the size and frequency of OCR?s enforcement efforts are on the rise, covered entities and business associates should heed OCR?s advice and ensure the regular conduct of risk analyses and risk management is incorporated into their compliance programs.

Related People