Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Record $5.5M HIPAA Deal Foreshadows Future Enforcement

Law360, New York (August 23, 2016, 1:06 PM ET) --

Stephanie A. Cason

On Aug. 8, 2016, the U.S. Department of Health and Human Services Office of Civil Rights issued the largest Health Insurance Portability and Accountability Act settlement to date with Advocate Health Care System. Advocate agreed to pay $5.55 million to settle a variety of HIPAA violations. Advocate is the largest health system in Illinois and operates more than 400 sites of care with 12 acute care hospitals. This settlement comes in the wake of a series of recent HIPAA violation settlements and other enforcement activities by the OCR, including phase two of the HIPAA audit program.

The Advocate settlement resulted from three separate HIPAA breach incidents reported by Advocate to HHS in connection with one of Advocate's wholly owned subsidiaries, Advocate Medical Group (AMG). The incidents occurred between August and November of 2013. The first incident involved the theft of four desktops from one of AMG's offices containing patient records. The second incident, occurring sometime between June 30 and Aug. 15, involved the breach of electronic protected health information (ePHI) of AMG patient data by a subcontractor billing company. The third involved the theft of an unencrypted laptop from the car of an AMG employee containing patient files with ePHI.

The three incidents combined involved the compromise of over 4 million individual patient records including names, addresses, dates of birth, credit card numbers with expiration dates, demographic information, clinical information and health insurance information.

Through an investigation of these incidents, OCR determined that Advocate failed to comply with HIPAA in a variety of ways; including the following:

- Failing to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to all of its ePHI;
- Failing to implement policies and procedures and facility access controls to limit physical access to the electronic information systems housed within a large data support center;
- Failing to obtain satisfactory assurances in the form of a written business associate contract that its business associate would appropriately safeguard all ePHI in its possession or control;

- Impermissibly disclosing the ePHI of 2,027 individuals when it failed to obtain business associate agreements prior to disclosure; and

- Failing to reasonably safeguard an unencrypted laptop when left in an unlocked vehicle overnight.

The settlement agreement outlines a corrective action plan for a period of two years and requires Advocate to implement numerous corrective actions to remedy the described failures. Corrective actions required by this plan include: modifying Advocate's existing risk analysis and providing a comprehensive risk analysis to HHS within 180 days for review and approval; developing and implementing a risk management plan and providing such plan to HHS for approval; implementing a process for evaluating environmental and operational changes; reviewing and revising policies and procedures on device and media controls; developing an encryption report which includes an inventory of devices and equipment that may access, store, download or transmit ePHI and evidence of encryption or an explanation why encryption is not necessary; reviewing and revising policies and procedures on device and media controls; reviewing and revising policies and procedures on facility access controls; reviewing and revising policies and procedures related to business associates; and developing an enhanced privacy and security awareness training program.

Advocate is also required to conduct internal monitoring of its compliance with the corrective action plan in addition to engaging an independent third-party assessor to review Advocate's compliance with the corrective action plan. The independent reviewer will provide reports of Advocate's compliance directly to HHS for review.

In announcing this settlement, the OCR outlined that this record-setting settlement amount was due to the extent and duration of the alleged noncompliance (with some of Advocate's violations existing since the inception of the security rule); involvement of the state attorney general in a corresponding investigation; the number of individuals whose ePHI was involved; and the size of Advocate itself. This settlement, along with the recent large settlements involving the other health systems and the first ever settlement against a business associate, highlights the increase in recent enforcement actions and the increase in penalty amounts being issued. The OCR has entered into settlement agreements in the past few months for increasing amounts of $650,000; $2.7 million; $2.75 million; and finally the Advocate settlement of $5.5 million.

Settlements such as this are likely to continue to be frequent especially considering that the OCR began phase two of the HIPAA audit program in March of this year. The OCR outlined that the phase two HIPAA audit program will evaluate the compliance of both covered entities and their business associates with the requirements of the HIPAA privacy, security and breach notification rules.

A first wave of covered entities have been selected for desk audits and the OCR has recently published guidance materials regarding phase two audits including a comprehensive list of questions that must be answered by those selected for review. Business associates and covered entities not selected for this first round of audits should be prepared for additional rounds of audits to occur as the OCR has made it clear this is the first step in the start of additional reviews of HIPAA compliance.

Both covered entities and business associates should review existing HIPAA compliance to avoid being subject to similar penalties as Advocate. Proactive HIPAA compliance efforts can ensure that

organizations are able to successfully complete a potential OCR audit and mitigate the risk of future losses due to HIPAA violations and breaches. Organizations should:

- Perform a risk assessment audit periodically: Failure to conduct a risk assessment audit has been a key factor in many recent HIPAA settlements and will be a focus of any future compliance reviews conducted by the OCR;

- Review and update policies and procedures as necessary: Outline appropriate policies and educate workforce members about appropriate procedures in order to ensure compliance;

- Encrypt ePHI at rest and in transmission: Although encryption is not required by HIPAA, it is highly recommended and serves as a safe harbor for reporting a HIPAA breach;

- Prepare breach response protocol before breaches occur: Ensure the breach response policies and procedures are in place that accurately reflect legal compliance requirements and ensure employees are aware of what to do when an incident occurs; and

- Ensure adequate insurance is in place to cover breach events and related liability: Costs for HIPAA breaches and related incidents can quickly become high and as cybersecurity incidents increase companies should ensure adequate coverage exists.

—By Stephanie A. Cason, Cooley LLP

Stephanie Cason is an associate in the health care and life sciences regulatory group at Cooley in Washington, D.C.