Published on *The National Law Review* https://natlawreview.com

Orthopedic Clinic Settles with HHS OCR for $1.5 Million over Claims of Systemic HIPAA Noncompliance

Article By:

Glenn A. Brown

The US Department of Health and Human Services' Office for Civil Rights ("OCR") recently announced a settlement with Georgia-based Athens Orthopedic Clinic PA (the "Clinic") to resolve multiple alleged violations of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act ("HIPAA").\

Under the terms of the settlement, the Clinic agreed to pay $1.5 million to OCR and to adopt a corrective action plan to settle potential violations of the Privacy and Security Rules under HIPAA. The Clinic provides orthopedic services to approximately 138,000 patients annually.

The Clinic had been notified by a journalist in June 2016 that a database of the electronic protected health information ("ePHI") of Clinic patients had been offered for sale on the dark web by a group known for infiltrating systems, stealing personal information, and issuing demands for payment to prevent the sale of data. Two days later, the group contacted the Clinic and demanded money in return for a complete copy of the database of the ePHI it had exfiltrated. The Clinic subsequently determined that the group had used a vendor's credentials to access their electronic medical record system to access and exfiltrate ePHI for over a month. The Clinic reportedly refused to pay the ransom.

The Clinic reported the breach to OCR in July 2016, informing OCR that 208,557 individuals were affected and that the ePHI disclosed included patients' names, dates of birth, social security numbers, medical procedures, test results and health insurance information.

According to the OCR press release, OCR's investigation discovered longstanding, systemic noncompliance by the Clinic with the HIPAA Privacy and Security Rules, including failures to conduct risk analyses, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with three of its business associates, and provide HIPAA Privacy Rule training to employees. As a result of these compliance failures, the Clinic failed to prevent unauthorized access to ePHI, in violation the HIPAA Security Rules.

In addition to the financial penalty, the Clinic agreed to a corrective action plan with a term of two years and covering the aspects of noncompliance discovered during OCR's investigation. The corrective action plan includes a requirement to obtain OCR's prior approval of policies, analyses

and training and to submit annual reports to OCR. In settling the matter, the Clinic made no admission of liability.

“Hacking is the number one source of large health care data breaches. Health care providers that fail to follow the HIPAA Security Rule make their patients’ health data a tempting target for hackers,” said OCR Director Roger Severino.

National Law Review, Volume X, Number 269