SHUMAKER

Client Alert

Business Information for Clients and Friends of Shumaker, Loop & Kendrick, LLP

09.21.2020

The OCR Gives Practices 1.5 Million Reasons to Prioritize HIPAA Compliance

Mary B. Ramsay, Associate | mramsay@shumaker.com | 843.996.1918
Grant P. Dearborn, Senior Attorney | gdearborn@shumaker.com | 813.227.2223

Today the Office of Civil Rights (OCR) at the U.S. Department of Health and Human Resources announced that a Georgia orthopedic clinic agreed to pay $1.5 million and adopt a two-year corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules.

Athens Orthopedic Clinic PA (the Practice), an orthopedic clinic that provides services to approximately 138,000 patients annually, was contacted by a hacker on June 28, 2016, who demanded money in return for a complete copy of the Practice database it stole. Upon investigation, the Practice determined that the hacker used a vendor's credentials on June 14, 2016, to access their electronic medical record system and "steal" patient health data.

On July 29, 2016, the Practice filed a breach report informing the OCR that 208,557 individuals were affected by the breach and that the Protected Health Information (PHI) disclosure included patient names, dates of birth, social security numbers, medical procedures, test results, and other health insurance information.

Despite the fact that the breach was a result of a cybercriminal and potentially an error by a non-employed individual, OCR's investigation discovered longstanding, systemic noncompliance with the HIPAA Privacy and Security Rules, including failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreement with multiple business associates, and provide HIPAA Privacy Rule training to workforce members.

The OCR's message is clear; patient health data is a tempting target for hackers and practices are responsible for ensuring its security by complying with HIPAA. The resolution agreement and corrective action plan may be found at https://www.hhs.gov/sites/default/files/athens-orthopedic-ra-cap.pdf.

Each health care entity that receives, maintains, creates, or interacts with PHI, should have Privacy & Security Policies, appoint an individual to be specifically responsible for Privacy & Security, conduct an annual risk assessment with results reported to leadership, timely investigate reports of breaches, maintain business associate agreements, have a formal process for granting anyone access to systems that contain PHI, and provide training to all individuals who have access to your PHI. If you have questions about any of these items, you should consult an experienced health care lawyer. The OCR has been assertive about its enforcement authority and this is only likely to continue.

To receive the latest legal and legislative information straight to your inbox, subscribe here.

This is a publication of Shumaker, Loop & Kendrick, LLP and is intended as a report of legal issues and other developments of general interest to our clients, attorneys and staff. This publication is not intended to provide legal advice on specific subjects or to create an attorney-client relationship.