FOR IMMEDIATE RELEASE
September 21, 2020

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Orthopedic Clinic Pays $1.5 Million to Settle Systemic Noncompliance with HIPAA Rules

Athens Orthopedic Clinic PA ("Athens Orthopedic") has agreed to pay $1,500,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. Athens Orthopedic is located in Georgia and provides orthopedic services to approximately 138,000 patients annually.

On June 26, 2016, a journalist notified Athens Orthopedic that a database of their patient records may have been posted online for sale. On June 28, 2016, a hacker contacted Athens Orthopedic and demanded money in return for a complete copy of the database it stole. Athens Orthopedic subsequently determined that the hacker used a vendor's credentials on June 14, 2016, to access their electronic medical record system and exfiltrate patient health data. The hacker continued to access protected health information (PHI) for over a month until July 16, 2016.

On July 29, 2016, Athens Orthopedic filed a breach report informing OCR that 208,557 individuals were affected by this breach, and that the PHI disclosed included patients' names, dates of birth, social security numbers, medical procedures, test results, and health insurance information.

OCR's investigation discovered longstanding, systemic noncompliance with the HIPAA Privacy and Security Rules by Athens Orthopedic including failures to conduct a risk analysis, implement risk management and audit controls, maintain HIPAA policies and procedures, secure business associate agreements with multiple business associates, and provide HIPAA Privacy Rule training to workforce members.

"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.

In addition to the monetary settlement, Athens Orthopedic has agreed to a robust corrective action plan that includes two years of monitoring. The resolution agreement and corrective action plan may be found at https://www.hhs.gov/sites/default/files/athens-orthopedic-ra-cap.pdf - PDF*.

* People using assistive technology may not be able to fully access information in this file. For assistance, contact the HHS Office for Civil Rights at (800) 368-1019, TDD toll-free: (800) 537-7697, or by emailing OCRMail@hhs.gov.

###

https://www.hhs.gov/about/news/2020/09/21/orthopedic-clinic-pays-1.5-million-to-settle-systemic-noncompliance-with-hipaa-rules.html