GT GreenbergTraurig

Alert | Health Care & FDA Practice/Data, Privacy & Cybersecurity

e

October 2020

OCR Imposes Fines on Health Plan, Business Associate, and Physician Group Related to Hacking Incidents; Warns Providers of Malware Attack.

In September, the Office for Civil Rights (OCR) announced three separate enforcement actions, including the second largest HIPAA monetary financial settlement in OCR history. These three actions and settlements were against: (1) a health plan; (2) a business associate; and (3) a physician group. All of these actions related to hacking and malware attacks on the entities in 2014 through 2016.

On Sept. 21, 2020, OCR announced a $1.5 million settlement with Athens Orthopedic Clinic, PA in Georgia. The settlement stemmed from an incident occurring on July 26, 2016, when a journalist notified the clinic that a database of their patient records was posted for sale on the internet. The posting of that patient data followed actions by a hacker who later contacted the clinic to demand a ransom for a complete copy of the stolen database. According to the OCR report, the hackers breached the clinic's systems using the credentials of a vendor on June 14, 2020, and were in the system for over a month during which time they exfiltrated the clinic's PHI.

The clinic reported the breach to OCR on July 29, 2016, and stated that 208,557 individuals had been affected. The breach involved the patients' names, dates of birth, social security numbers, medical procedures, test results, and health insurance information. OCR contended that the practice had

© 2020 Greenberg Traurig, LLP

longstanding and systemic noncompliance with HIPAA privacy and security rules, including the failure to conduct a risk analysis, implementation of risk management and audit controls, failure to maintain HIPAA policies and procedures, failure to secure business associate agreement with multiple vendors, and failure to provide training to workforce members.

In addition to the fines, the clinic agreed to a robust corrective action plan that includes two years of monitoring by OCR. The corrective action plan also includes analysis of security risks and vulnerabilities that incorporates all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by the clinic or its affiliates that contain, store, transmit, or receive ePHI.

A couple of days later, on Sept. 23, 2020, OCR announced that it had reached a settlement with a Business Associate (BA), CHSPSC LLC, for $2.3 million to settle a breach that affected approximately six million individuals. The BA provided IT and health information management services to hospitals and physician clinics owned by Community Health Systems and the incident affected multiple Covered Entities. In April 2014, the FBI notified the BA that its systems had been hacked and that it had traced a cyber-hacking group's advanced persistent threat to the BA's systems. The hackers allegedly continued to access and exfiltrate data until August 2014 using compromised administrative credentials to remotely access the BA's systems through its virtual private network.

OCR found that the BA demonstrated longstanding and systemic noncompliance with HIPAA security rules, including the failure to conduct a risk analysis and failures to implement information system activity review, security incident procedures, and access controls. The BA also agreed to a corrective action plan and two years of monitoring by OCR. The corrective action plan includes revision of policies and procedures regarding technical access controls for software applications and network equipment, information system activity review for the regular review of audit logs, access reports, and security incident tracking reports, Security Incident Procedures and Response and Reporting, and password management.

Finally, on Sept. 25, 2020, a health insurer, Premera Blue Cross, agreed to pay $6.85 million to settle a data breach that affected over 10.4 million people. This was the second biggest payment in OCR history to resolve a HIPAA investigation. The settlement stemmed from a March 17, 2015, breach report stating that hackers had gained access to its information technology system. The threat actors utilized a phishing email to install malware that gave them access to the system in May 2014. This improper access was not discovered until January 2015 during which time the actors gained access to names, addresses, dates of birth, email addresses, social security numbers, bank account information, and health plan clinical information.

OCR found that the health plan demonstrated systemic noncompliance with the HIPAA rules, including the failure to conduct an enterprise-wide risk assessment and the failure to implement risk management and audit controls. The health plan also agreed to a corrective action plan that includes two years of monitoring by OCR and an accurate and thorough Risk Analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

A key issue in all three settlements was the failure to have a comprehensive risk assessment and other security controls. All Covered Entities and Business Associates are required to conduct periodic risk analyses under the HIPAA security rules. Health care entities, and their Business Associates, should review their risk assessments and make sure they are being conducted on a regular basis.

Furthermore, health care providers and their Business Associates should make sure that malware detection and recovery from hacking attacks are part of their assessments.

© 2020 Greenberg Traurig, LLP

In line with the recent enforcement decisions, OCR recently issued a warning to health care providers about the Taidoor malware allegedly being used by the Chinese government, which has already affected certain health care systems. The warning also includes response actions and recommended mitigation techniques and reference a Malware Analysis Report (MAR) by the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the Department of Defense. More information on Chinese malicious cyber activity is available on the CISA website. CISA recommends taking the following actions:

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable file and printer sharing services. If these services are required, use strong passwords or active directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Authors

This GT Alert was prepared by:

- Mark L. Mattioli | +1 215.988.7884 | mattiolim@gtlaw.com
- Eleanor (Miki) A. Kolton | +1 202.331.3134 | koltonm@gtlaw.com
- Samantha R. Beck | +1 202.530.8540 | becks@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Germany.¬ Houston. Las Vegas. London.* Los Angeles. Mexico City.+ Miami. Milan.» Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul.∞ Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv.^ Tokyo.¤ Warsaw.~ Washington, D.C.. West Palm Beach. Westchester County.

This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about

*the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ¬Greenberg Traurig's Berlin office is operated by Greenberg Traurig Germany, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Santa Maria, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. ¤Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. ~Greenberg Traurig's Warsaw office is operated by Greenberg Traurig Grzesiak sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in Greenberg Traurig Grzesiak sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2020 Greenberg Traurig, LLP. All rights reserved.*