SAUL EWING ARNSTEIN & LEHR LLP

ALERT

Health Care Practice

MAY 2021

Clinical Laboratory Agrees to Pay $25,000 to Settle Potential HIPAA Security Rule Violations

Bruce D. Armon | Samatha R. Gross | Patricia Varona Garcia

On May 25, 2021, the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS), announced that Peachstate Health Management, LLC d/b/a AEON Clinical Laboratories (Peachstate) agreed to pay $25,000, enter into a Resolution Agreement, and adopt a Corrective Action Plan (CAP) to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Peachstate provides diagnostic and laboratory-developed tests, including clinical and genetic testing services. Peachstate is based in Georgia and is certified under the Clinical Laboratory Improvement Amendments of 1988 (CLIA). The Resolution Agreement is not an admission of liability by Peachstate.

In December 2017, OCR initiated a compliance review of Peachstate to determine its compliance with the HIPAA Privacy and Security Rules. The 'story' as to how OCR eventually decided to review Peachstate is instructive. In January 2015, the U.S. Department of Veterans Affairs (VA) reported a breach of unsecured protected health information (PHI) involving a program managed by its business associate, Authentidate Holding Corporation (AHC). In August, 2016, OCR initiated a compliance review of AHC to determine its compliance with the Privacy and Security Rules related to the VA breach. During the compliance review, the VA learned that AHC and Peachstate had earlier entered into a "reverse merger" in January, 2016, whereby AHC acquired Peachstate. OCR then decided to review the Peachstate clinical laboratories to assess their compliance with the HIPAA Privacy and Security Rules.

The OCR investigation concluded that Peachstate failed to conduct an enterprise-wide risk analysis and did not implement risk management and audit controls. Additionally, the investigation disclosed systemic noncompliance with the HIPAA Security Rule, and Peachstate failed to maintain documentation of HIPAA Security Rule policies and procedures.

In addition to the monetary settlement, Peachstate entered into a CAP that includes three (3) years of monitoring by HHS and a requirement to do each of the following:

- Conduct an enterprise-wide risk analysis of the security threats and vulnerabilities of all PHI created, received, maintained or transmitted, including all electronic media, workstations, and information systems owned, controlled or leased by Peachstate;
- Develop and implement a risk management plan to address and mitigate any security threats and vulnerabilities discovered during the risk analysis;
- Review and revise Peachstate's written policies and procedures, subject to HHS review and approval;
- Distribute the policies and procedures to all current members of the workforce, and to new members of the workforce within fifteen days of the beginning of service;

- Train all workforce members who have access to PHI on the revised policies and procedures within thirty days of adopting such policies and procedures;
- Promptly investigate reports of potential violations of the revised policies and procedures and, if a violation occurred, report such events to HHS; and
- Designate an individual or entity, to be a monitor and to review compliance with CAP.

This OCR settlement is an important reminder that all "clinical laboratories, like other covered health care providers, must comply with the HIPAA Security Rule and failure to implement basic Security Rule requirements make HIPAA-regulated entities attractive targets for malicious activity, and needlessly risks patients' electronic health information" as noted by Acting OCR Director Robinsue Frohboese. The settlement is also an important reminder that businesses involved in corporate mergers should ensure that each covered entity (and business associates) maintain HIPAA Privacy Rule and Security Rule compliance.

Saul Ewing Arnstein & Lehr attorneys regularly counsel and assist covered entities and business associates with HIPAA compliance, breach issues and workforce training. For more information relating to Saul Ewing Arnstein & Lehr's HIPAA compliance practice, please contact the authors or the attorney at the Firm with whom you are regularly in contact.

This alert was written by Bruce D. Armon, office managing partner of the Firm's Philadelphia office and chair of its Health Care Practice, Samantha R. Gross, a member of the Practice; and Patricia Varona Garcia, a member of the Firm's Corporate Practice. Bruce can be reached at (215) 972-7985 or at Bruce.Armon@saul.com. Samantha can be reached at (215) 972- 7161 or at Samantha.Gross@saul.com. Patricia can be reached at (312) 876-7156 or at Patricia.VaronaGarcia@saul.com. This alert has been prepared for information purposes only.

Did you find this information useful? Please provide your feedback here and also let us know if there are other legal topics of interest to you.