SAUL EWING ARNSTEIN & LEHR LLP

Alert

HEALTH CARE PRACTICE

NOVEMBER 2019

AUTHORS

BRUCE D. ARMON

LAUREN A. FARRUGGIA

SAMANTHA R. GROSS

Large New York State Health System Agrees To Pay $3 Million For Its Failure to Repeatedly Encrypt Mobile Devices

SUMMARY

On November 5, 2019, the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) announced a $3 million settlement with the University of Rochester Medical Center (URMC) to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules. URMC admitted no wrongdoing as part of the OCR settlement.

As part of the URMC Resolution Agreement, URMC will be subject to a two-year Corrective Action Plan (CAP).

In May 2013, URMC submitted a breach report to OCR because it lost an unencrypted flash drive containing electronic protected health information (ePHI) the previous month. In June 2013, OCR initiated an investigation surrounding URMC's HIPAA compliance. In January 2017, URMC again contacted OCR because one of its unencrypted laptops containing 43 patients' ePHI was stolen from a treatment facility. OCR initiated an additional HIPAA compliance investigation assessing URMC's practices. In 2010, OCR investigated URMC because of its loss of an unencrypted flash drive, and OCR provided technical assistance to URMC relating to HIPAA compliance.

As part of the two-year CAP, URMC agreed to each of the following:

- conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality and availability of ePHI and prepare and share with HHS a statement of work of its risk analysis;
- develop and implement a risk management plan, subject to HHS approval;
- develop a process to evaluate any environmental or operational changes that affect the security of URMC's ePHI;
- review and revise its Privacy and Security Rules Policies and Procedures to ensure HIPAA compliance;
- promptly investigate reported incidents related to its workforce members failing to comply with URMC's adopted, revised Policies and Procedures;
- provide HHS with training materials addressing the requirements of the Privacy, Security and Breach Notification Rules that will be used for appropriate workforce members;
- submit an implementation report and annual CAP compliance reports to OCR.

The OCR settlement is a critical – and costly – reminder for all HIPAA-covered entities that the obligation to safeguard ePHI includes the security of electronic hardware, including laptops, flash drives and cell phones that are used daily by HIPAA-covered entities and their workforce members.

This OCR settlement may be an example of three strikes and you are "out" given the 2010, 2013 and 2017 incidents affecting URMC. All covered entities should review their policies and processes to ensure they protect a patient's rights under HIPAA.

Saul Ewing Arnstein & Lehr attorneys regularly assist covered entities with creating and maintaining their HIPAA privacy policies and work with covered entities and business associates to ensure HIPAA Privacy Rule and Security Rule compliance. If you have questions regarding an issue raised in this post, 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, Lauren A. Farruggia and Samantha R. Gross, associates in the practice. Bruce can be reached at (215) 972-7985 or at Bruce.Armon@saul.com. Lauren can be reached at (202) 295-6671 or at Lauren.Farruggia@saul.com. Samantha can be reached at (215) 972-7161 or at Samantha.Gross@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.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute "Attorney Advertising."

COPYRIGHT © 2019 SAUL EWING ARNSTEIN & LEHR LLP, A DELAWARE LIMITED LIABILITY PARTNERSHIP. ALL RIGHTS RESERVED.