SAUL EWING ARNSTEIN & LEHR LLP

Alert

HEALTH CARE PRACTICE

OCTOBER 2019

AUTHORS

BRUCE D. ARMON

LAUREN A. FARRUGGIA

Multi-Hospital Florida Academic Medical Center Pays $2.15 Million Civil Money Penalty for Violating HIPAA Security and Breach Notification Rules, Including an NFL Player

SUMMARY

On October 23, 2019, the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS) announced that it had imposed a $2,154,000 civil money penalty (CMP) against a Miami-based health system for years-long violations of the Health Insurance Portability and Accountability Act (HIPAA) Security and Breach Notification Rules.

Jackson Health System (JHS) elected to pay the full CMP and waive its right to a hearing and declined to contest OCR's findings in its July 22, 2019 Notice of Proposed Determination. The Notice includes an explanation for the basis of the CMP, the factors OCR considered in determining the amount of the CMP, and a table demonstrating the actual calculations.

In August 2013, JHS submitted a breach report to OCR claiming that in January 2013 its health information management department lost records containing protected health information (PHI) of 756 patients. JHS' internal investigation ultimately determined that it lost additional patient records containing PHI in December 2012, bringing the grand total to 1,456 affected patients, but JHS did not report this additional loss to OCR until June 7, 2016.

OCR began investigating JHS in July 2015 after a reporter posted a photograph on social media of a JHS operating screen bearing a patient's PHI – the patient was a National Football League player. Through the course of its investigation, OCR determined that two JHS employees had accessed NFL players' electronic medical records with no job-related purpose. In February 2016, JHS submitted another breach report to OCR, stating that a JHS employee had accessed over 24,000 patient records since 2011 and had sold patient PHI.

OCR concluded in its Notice of Proposed Determination that JHS failed to:

- Provide timely and accurate breach notification to HHS;
- Conduct an appropriate enterprise-wide risk analysis;
- Manage and remediate identified risks to a reasonable and appropriate level;
- Implement policies and procedures to prevent, detect, contain and correct HIPAA Security Rule violations;
- Regularly review information system activity records; and
- Restrict authorization of its workforce members' access to patient PHI to the minimum necessary to accomplish their job duties.

This CMP is a costly reminder for all HIPAA-covered entities of the importance of timely breach notifications to HHS and of the obligation to restrict workforce access to patient PHI, especially when high-profile individuals are being treated by a HIPAA covered entity. All covered entities should review their policies and processes to ensure that they protect a patient's rights under HIPAA – the Privacy, Security, and Breach Notification Rules – and should revise internal risk assessment and system activity mechanisms if needed.

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 compliance with the HIPAA Privacy, Security, and Breach Notification Rules. 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, chair of the Firm's Health Care Practice and Philadelphia office managing partner, and Lauren A. Farruggia, an associate 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.
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.