KRIEG DEVAULT

Insights

OCR Throws Penalty Flag on Jackson Health System's Multiple HIPAA Violations

December 2, 2019

By: Stacy Walton Long and

The Office of Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) recently announced that it imposed $2,154,000 in civil money penalties (CMPs) against Jackson Health System ("Jackson") for multiple violations of the Security and Breach Notification Rules of the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA), including records relating to an NFL football player.

In July 2015 multiple media reports disclosed the medical records of a Jackson patient and well-known NFL player who had a finger amputated at the hospital. The reports included a photograph of the patient's record on an electronic display located in a Jackson operating room, along with a paper schedule containing the patient's protected health information (PHI). Jackson's investigation further revealed that two of its employees accessed the NFL player's electronic medical record without a job-related purpose, in violation of HIPAA.

Previously, Jackson filed a breach report in August of 2013 notifying OCR that its Health Information Management Department lost the paper records of 756 patients containing PHI. Although Jackson complied with HIPAA's reporting requirement after this breach, Jackson's internal investigation revealed three additional boxes of patient records that were lost which affected 680 additional patients. Jackson did not amend its breach report or notify OCR of this additional loss until June 2016.

A final violation occurred in February 2016 when Jackson submitted a breach report to OCR indicating that a Jackson employee had improperly accessed the records of 24,188 patients since 2011. The report also revealed that the same employee had sold patients' information. Jackson's failure to discover the breach was the result of inadequate risk analyses and insufficient restriction of the employee's access to PHI.

In determining the amount of civil money penalties (CMPs), OCR considered the nature and extent of the violations, the nature and extent of the harm resulting from the violations, the history of Jackson's compliance, Jackson's financial condition, and Jackson's cooperation in the investigation.[1] OCR provided the amount of CMPs per violation:

- $328,000 for violating the Information Access Management;[2]
- $326,000 for violating the Security Management Process;[3]and
- $1,500,000 for violating the Notification Rule under HIPAA.[4]

Jackson could have likely avoided the multiple violations, or at a minimum mitigated the risks of the violations, had it taken preventive measures. Health care providers should learn from Jackson's mishaps by implementing enterprise-wide risk analyses, risk management policies, and processes to restrict employees' access to PHI.

If you have questions regarding HIPAA compliance policies, or other HIPAA-related questions, please contact Stacy Walton Long, Alexandria M. Foster, or any other Krieg DeVault attorney in the Health Care Practice Group.

[1] https://www.hhs.gov/sites/default/files/jackson-health-system-notice-of-proposed-determination_508.pdf

[2] 45 C.F.R. § 164.308(a)(4); amount based on 45 C.F.R. § 164.404(b)(2)(ii).

[3] 45 C.F.R. § 164.308(a)(1); amount based on 45 C.F.R. § 164.404(b)(2)(ii).

[4] 45 C.F.R. § 164.408; amount based on 45 C.F.R. § 164.404(b)(2)(ii).