KRIEG DEVAULT

Insights

Failure to Terminate Access to PHI Leads to HIPAA Violation

December 17, 2018

By: Stacy Walton Long and Alexandria M. Foster

The Health and Human Services' Office of Civil Rights ("OCR") recently entered into a Resolution Agreement with Pagosa Springs Medical Center ("PSMC"), resolving HIPAA violations over five years after the initial investigation began.[1] On June 7, 2013, OCR initiated an investigation that revealed PSMC failed to terminate a former employee's remote access to PSMC's web-based scheduling calendar. The calendar, managed by one of PSMC's vendors (the "Vendor"), contained patients' electronic protected health information ("ePHI"). OCR's investigation revealed that PSMC impermissibly disclosed the ePHI of at least 557 patients to the former employee and to the Vendor.

As with many other HIPAA breach investigations, OCR discovered that PSMC did not have a business associate agreement with the Vendor, which is an obvious violation of HIPAA.[2] Further, PSMC's failure to de-activate the former employee's username and password allowed the individual to continue accessing ePHI after PSMC terminated the individual.

The terms of the Resolution Agreement required PSMC to pay OCR $111,400 and enter into a two year Corrective Action Plan. The Corrective Action Plan requires PSMC to, among other things, revise its policies and procedures relating to business associates; assess its policies and procedures relating to uses and disclosures of ePHI; provide revised training to its workforce members regarding, in part, privacy and security awareness; and conduct a thorough risk analysis and risk management plan to comply with HIPAA standards. To see the complete Resolution Agreement and the Corrective Action Plan attached thereto, please click here.

It is critical that health care providers are fully aware of those who have access to protected health information at all times. This includes ensuring that proper procedures are in place to terminate access to such information, when appropriate, with former employees, vendors, and any other individual or entity who may have access to ePHI. Lastly, covered entities must always enter into business associate agreements with business associates before sharing any ePHI, as required under HIPAA.[3]

If you have questions regarding HIPAA compliance policies or issues, business associate agreements, or other HIPAA-related questions, please contact Stacy Walton Long at slong@kdlegal.com, Alexandria M. Foster at afoster@kdlegal.com, or any other Krieg DeVault attorney in the Health Care Practice Group.

1. https://www.hhs.gov/about/news/2018/12/11/colorado-hospital-failed-to-terminate-former-employees-access-to-electronic-protected-health-information.html.
2. See 45 C.F.R. § 164.502(e), § 164.308(b), and § 164.314(a)
3. Id.