COSMOS
Navigate the Compliance Universe

Compliance Today - June 2019
Knowing who has access to your PHI and who does not

By Jay P. Anstine

Jay P. Anstine (jay.anstine@bannerhealth.com) is the Area Compliance Program Director for Banner Health's Western Region Rural Hospitals, based in Greeley, CO.

On December 11, 2018, the Department of Health and Human Services, Office for Civil Rights (OCR) announced a settlement with a critical access hospital in Colorado, Pagosa Springs Medical Center (PSMC),[1] which agreed to pay $111,400 to resolve alleged violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

According to the settlement, OCR alleged that from July to September of 2013, PSMC impermissibly disclosed the protected health information (PHI) of 557 individuals. The cause of the impermissible disclosures was attributable to two sources. First, the hospital failed to deactivate a former employee's credentials to access a web-based scheduling calendar. Additionally, through the course of the investigation, it was discovered that PSMC did not have a business associate's agreement (BAA) with Google, the contracted vendor providing the software.

This recent settlement highlights some important reminders when it comes to knowing who has access to your PHI.

Important reminders

- **There are no small fish.** PSMC is a critical access hospital (i.e., 25 beds or less) located in a rural part of Colorado. Similar to the Allergy Associates of Hartford PC settlement from November 2018, this case is a cautionary tale that no organization is too small for OCR's resources to investigate.
- **Security management extends after employment.** In this case, PSMC failed to remove a former employee's access after separation of employment. This settlement is a reminder that security management doesn't end when the employee leaves the building for the last time.
- **When it comes to BAAs, watch out for yourself—and others.** If you've ever taught a teenager to drive, chances are you've screamed, "Drive defensively!" when you notice another driver not paying attention. In the context of protecting your organization's PHI, you need to contract defensively too. What is interesting is that unlike PSMC, Google is not a small organization. To that end, don't assume the other party is following the rules of the road and catching the relationships necessitating a BAA.

As with any OCR settlement, it is unfortunate the events occurred, but they do provide us with helpful reminders. For example, review your policies or find out if you have any internal control deficiencies or communication gaps. You can also use this settlement to educate your workforce members to prevent similar occurrences in your organization.

1 HHS Office for Civil Rights Settlement with Pagosa Springs Medical Center (PSMC), November 5, 2018.

https://bit.ly/2GiAeSK