First HIPAA Breach Notification Enforcement Ends in Settlement Against Tardy Health System

One might think the U.S. Department of Health and Human Services (HHS has been around too long to experience any “firsts.” But the Office for Civil Rights (OCR) under the HHS has recently done just that when it settled the first Health Insurance Portability and Accountability Act (HIPAA) enforcement action for untimely notification regarding a privacy breach.

The HIPAA Breach Notification Rule insists that time is of the essence for healthcare organizations to report incidents that might compromise patients’ protected health information (PHI). Specifically, the institution that suffered the breach must notify concerned parties (and, if more than 5oo individuals are affected, prominent media outlets as well) within 60 days of the event’s discovery.

While the rule that demands that brand of timeliness may seem arbitrary or even soft around the edges, the OCR’s recent settlement should give pause to health institutions that might not have taken HIPAA breach notification expediency all that seriously before now.

Presence Health loses track of PHI for several hundred individuals

The OCR received a report of a potential breach from Presence Health on January 31, 2014. The Chicago-based health system said that on October 22, 2013 it realized that hardcopy records involving more than 800 patients’ PHI were unaccounted for (lost or perhaps stolen) at the company’s surgery center in the Presence St. Joseph Medical Center in Joliet, Illinois. Among the sensitive information included in the missing documents: individuals’ names, dates of birth, dates of medical care, types of procedures, names of surgeons, and more.

The ensuing OCR investigation determined that the health system did not notify all of the patients involved, the OCR, and media outlets within the 60 days post-discovery stipulated under HIPAA.

Presence acknowledged the delay, but blamed it on “miscommunication” between staff members. That explanation failed to soften the OCR’s position—the tardiness in notification ultimately left the potentially compromised individuals unaware (and therefore potentially vulnerable), for a longer period than was acceptable.

OCR Director Jocelyn Samuels had this to say: “Covered entities need to have a clear policy and procedures in place to respond to the Breach Notification Rule’s timeliness requirements. Individuals need prompt notice of a breach of their unsecured PHI so they can take action that could help mitigate any potential harm caused by the breach.”

Presence will be nearly $.5 mil lighter once settlement is paid

The enforcement action against Presence has ended in a settlement of $475,000 against the health plan. Further, Presence must immediately take steps to make it compliant with the HIPAA Breach Notification Rule (this includes mandatory training for employees on the company's breach reporting protocol, as well as a revision to its current procedures to bring them in line with what OCR requires).

The seriousness with which the OCR views this issue is reflected in the relatively steep settlement figure for a relatively few individuals affected.

Still, it's not a stratospheric settlement. The HHS explains on its website:

"With this settlement amount, OCR balanced the need to emphasize the importance of timely breach reporting with the desire not to disincentive breach reporting altogether."

For more information/questions regarding any legal matters, please email info@nelsonhardiman.com or call 310.203.2800.