COSMOS
Navigate the Compliance Universe

Report on Medicare Compliance Volume 30, Number 11. March 22, 2021

Before It's Too Late: Ensuring BA, Subcontractor Compliance

By Theresa Defino

Sometime during the fall, a worker for a subcontractor of Humana Inc. decided to share member information from medical records via a Google document with people he was training to be medical coders, part of his attempt to run a "personal coding business endeavor."[1]

Early last month, Humana had to notify 65,000 individuals, multiple state officials, the press and the HHS Office for Civil Rights (OCR) of the worker's data breach. In its notification, Humana said unauthorized access continued from October to December before it was discovered by the now-former worker's employer, which Humana said is named Visionary. Technically, Visionary is (or was—current status isn't clear) a subcontractor for a company called Cotiviti, which Humana uses to develop risk adjustment scores needed for payment of certain members. Cotiviti is a business associate (BA) of Humana, the covered entity (CE).

Around the same time, Accellion Inc. was informing its clients that hackers had accessed its file transfer system[2] —among them a big law firm whose exposed documents included prescriptions written for hundreds of patients, including their names.

HIPAA compliance officials know that patient data must be safeguarded everywhere it resides and when it travels from CEs to BAs and then on to subcontractors. As these recent incidents show, the ties that bind these organizations are crucial to ensuring proper notifications in the event of a breach.

But how can CEs be certain that BAs and subcontractors will perform well after an unauthorized disclosure and, in general, be compliant during their usual handling of protected health information (PHI)?