KRIEG DEVAULT

Insights

Failure To Have A Business Associate Agreement Could Be A $31,000 Mistake

May 17, 2017

By: Stacy Walton Long

FileFax, Inc. ("FileFax") is a Business Associate of the Center for Children's Digestive Health ("Center"). The Center is a small, for-profit healthcare provider with a subspecialty practice in pediatrics. Since 2003, FileFax stored inactive paper medical records that contained protected health information ("PHI") for patients of the Center.

On August 13, 2015, the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR") conducted a compliance review of the Center to determine whether the Center's disclosure of PHI to FileFax was permissible under the Privacy Rule. When neither party could produce a signed Business Associate Agreement ("BAA") prior to October, 2015, OCR determined that the Center impermissibly disclosed the PHI of at least 10,728 individuals to FileFax when the Center transferred the PHI to its Business Associate without obtaining a signed Business Associate Agreement with FileFax. Pursuant to 45 C.F.R. Section 164.502(e), the Center is required to obtain satisfactory assurances from FileFax, in the form of a written BAA, that FileFax would appropriately safeguard the PHI that was in FileFax's possession or control.

As a result, the Center settled its potential violations of HIPAA by paying OCR $31,000, and agreed to implement a Corrective Action Plan ("Plan"). The Plan requires, among other things, the Center to develop, maintain, and revise its written policies and procedures to comply with the HIPAA standards that govern the privacy and security of individually identifiable health information[1]. For the complete Plan, please click here.

[1] *See* 45 C.F.R. Part 160 and Subparts A, C, and E of Part 164, the Privacy and Security Rules.