KAUFMAN | DOLOWICH

Mansfield Rule Certified 2022-2023

Partner Avery Dial quoted in article, " Medicare MOVEit breach a warning of persistent cyber-danger; watch impact," Part B News, 8-21-2023

A data breach at a Medicare subcontractor is bad news for affected beneficiaries — and a warning to practices that downstream providers may also be putting their files in danger.

A July 28 press release from HHS and CMS announced that they had "responded" to a "May 2023 data breach Progress Software's MOVEit Transfer software on the corporate network of Maximus Federal Services, Inc. (Maximus), a contractor to the Medicare program, that involved Medicare beneficiaries' personally identifiable information (PII) and/or protected health information (PHI)."

This Maximus incident is only part of a massive breach suffered by file transfer producer MOVEit, consequences of which are still rolling out. Some of the victims are health care entities, such as Colorado's Medicaid administration, whose breach potentially exposed the data of 4 million beneficiaries; some are education entities such as the New York City Department of Education and UCLA; other are corporations such as Siemens.

Avery A. Dial, chair of the Data Privacy & Cybersecurity Practice Group at Kaufman Dolowich LLP in Fort Lauderdale, Fla., notes one ominous aspect of the MOVEit breach: while its total market share isn't huge, "it does have almost 100% of federal civilian agencies and U.S. military agencies."

Maximus is a qualified independent contractor (QIC), a type of contractor that usually handles Medicare appeals at the reconsideration or second level. HHS believes the breach has affected 612,000 current Medicare beneficiaries. See file for full article

Part B News - 08-21-23 - Medicare MOVEit breach a warning - Avery Dial quoted