

Business Associate Failed to Safeguard 3.5 Million Patients' Medical Records

Drinker Biddle®

Article By

[Sumaya M. Noush](#)

[Drinker Biddle & Reath LLP](#)

[DBR on Data](#)

- [Health Law & Managed Care](#)
- [Administrative & Regulatory](#)
- [All Federal](#)

Tuesday, May 28, 2019

Medical Informatics Engineering, Inc. and its wholly-owned subsidiaries (MIE) and the Office for Civil Rights at the U.S. Department of Health and Human Services (HHS-OCR) entered into a \$100,000 settlement and two-year corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA).

On July 23, 2015, MIE filed a HIPAA breach report with HHS-OCR upon discovering that hackers accessed the electronic protected health information (ePHI) of approximately 3.5 million individuals. MIE discovered suspicious activity on one of its servers on May 26, 2015, and further learned that the hackers gained unauthorized access beginning May 7, 2015. In addition to determining the impermissible disclosure of 3.5 million individuals' ePHI, HHS-OCR further concluded that MIE failed to conduct an accurate and thorough risk analysis of its potential risk and vulnerabilities to the confidentiality, integrity, and availability of its ePHI.

As a reminder, business associates are directly obligated to comply with the HIPAA Security Rule. Business associates must conduct and document a risk analysis of their information systems to identify potential security risks and respond appropriately. Business associates should also routinely review and update their risk analyses. HHS-OCR has provided a sample risk assessment tool that is freely available to covered entities and business associates alike.

Source URL: <https://www.natlawreview.com/article/business-associate-failed-to-safeguard-35-million-patients-medical-records>