

MAY 2019

**AUTHORS**

BRUCE D. ARMON  
KARILYNN BAYUS

# Hacked Business Associate Agrees to Pay \$100,000 as Part of HIPAA Settlement

## SUMMARY

On May 23, 2019, the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), [announced that Medical Informatics Engineering, Inc. \(MIE\) agreed to pay \\$100,000 to settle alleged HIPAA violations that exposed the protected health information \(PHI\) of more than 3,500,000 individuals when hackers accessed its servers in an unauthorized manner.](#)

MIE is a HIPAA business associate based in Indiana that provides software and electronic medical record services to health care providers.

According to the OCR press release announcing MIE's settlement, MIE filed a HIPAA breach report in July, 2015 "following discovery that hackers used a compromised user ID and password to access the electronic protected health information (ePHI) of approximately 3.5 million people."

In addition to the \$100,000 payment, MIE entered into a two-year corrective action plan (CAP) with HHS. As part of the CAP, MIE agreed to:

- Conduct a comprehensive risk analysis of "the potential risks and vulnerabilities to the confidentiality, integrity, and availability" of MIE's ePHI within 30 days of the effective date of the OCR settlement. OCR specified MIE's risk analysis shall include an inventory of its facilities and categories of electronic equipment;
- Develop and implement a written risk management plan to address and mitigate security risks and vulnerabilities identified in the risk analysis; and
- Provide annual reports to HHS of its compliance efforts with respect to the CAP.

The MIE settlement highlights the importance of covered entities and business associates conducting thorough risk analyses as required by the Security Rule. MIE is a HIPAA business associate, and so the settlement also serves as a reminder that business associates have direct liability to the government under HIPAA. Hackers are pervasive in the health care delivery system (and across all industries) and MIE's failure to identify potential risks and vulnerabilities to its ePHI resulted in an expensive settlement for MIE.

Saul Ewing's health law practitioners regularly assist HIPAA-covered entities and business associates with HIPAA compliance issues, including preparing incident response and breach notification plans and advising clients who experience a security incident or potential HIPAA breach. For more information, contact the authors of this Alert.

This Alert was written by Bruce D. Armon, Chair of the Firm's Health Care Practice and Managing Partner of the Philadelphia office, and Karilynn Bayus, Vice Chair of the Firm's Health Care Practice. Bruce can be reached at 215-972-7985 or [bruce.armon@saul.com](mailto:bruce.armon@saul.com). Karilynn can be reached at 215-972-1892 or [karilynn.bayus@saul.com](mailto:karilynn.bayus@saul.com). This publication has been prepared for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute "Attorney Advertising."