Codify
BY AAPC

Health Information Compliance Alert

Case Study: Settlement Equals Hiccup for BA's Big Breach

Is this indicative of things to come?

A recent case illustrates why business associates (BAs) aren't exempt from HIPAA enforcement, but the results of the settlement are more of a whimper than a bang. However, with new federal BA liability guidance on the table, some entities may get mixed messages on compliance - leading to treacherous waters and more headaches down the line.

Background: Last month, the Indiana-based software and EMR firm **Medical Informatics Engineering, Inc.** (MIE) settled for $100,000 with the **Department of Health and Human Services Office for Civil Rights** (OCR) for "potential" HIPAA violations related to a hacking incident, a release indicates. The breach, which occurred on May 7, 2015, concerned unauthorized access due to the combination of a compromised username and password.

The cyberattack at MIE impacted the electronic protected health information (ePHI) of about 3.5 million individuals. The BA failed to analyze its risks properly, making the organization ripe for a cyber attack, according to an OCR investigation performed after the breach. In this case, a risk analysis and better security education on usernames and passwords might have alleviated the problem (see advice, p.44).

"Entities entrusted with medical records must be on guard against hackers," warns **Roger Severino,** OCR director, in a release. "The failure to identify potential risks and vulnerabilities to ePHI opens the door to breaches and violates HIPAA."

MIE must also follow a Corrective Action Plan (CAP) for the next two years with requirements to conduct a risk analysis and then implement risk management protocols with OCR's approval.

See the CAP at www.hhs.gov/sites/default/files/mie-ra-cap.pdf.

BA's Settlement Amounts to Smaller Than Expected Fine

Perhaps, the OCR is feeling more charitable toward BAs, as it rarely publishes HIPAA violation details of BA breaches, instead focusing on covered entities (CEs). Or, maybe the minor settlement signals a nod to the reduced HIPAA Civil Monetary Penalty (CMP) annual limit caps that were updated in the Federal Register in April (see Health Information Compliance Alert, Vol. 19, No. 5).

Whatever the reasoning, the settlement seems out of character for the OCR. "I think it is total head-scratcher," says Richmond, Virginia-based attorney **Nathan A. Kottkamp,** of national law firm **McGuire Woods LLP**.

Kottkamp continues, "I really don't know if there is some non-public backstory on why the settlement is so low that specifically relates to the financial status of MIE or whether this is the first of a kinder, friendly OCR."

"The consequences of the incident, in terms of the numbers affected and information disclosed, and past resolution agreements suggest that the amount of the penalty might have been higher under prior limits, and that the OCR may have exercised judgment based on MIE's culpability," adds Philadelphia-based attorney **Edward I. Leeds**, of national law firm **Ballard Spahr LLP**.

Interestingly, the OCR released a BA liability fact sheet on May 24 - the day after it published the MIE settlement particulars. The fact sheet stands as a solemn reminder to BAs that the feds will pursue enforcement for failure to live up to their part in HIPAA compliance.

CMP Annual Limits May Have Factored Into Results

The details are slim concerning the OCR's decision making on this case. Neither the OCR release nor the resolution agreement offer much in the way of specifics on the MIE settlement. However, the $100k penalty lines up with the new CMP limits, which adds another layer to the settlement.

"The fact that the amount of the penalty exactly matches the new maximum penalty for any one type of violation when there is reasonable cause suggests that the new limits or - depending on when the resolution agreement was actually reached - the prospect of new limits may have had an influence on this matter," Leeds acknowledges.

In the end, the "modest" federal fine may have been the end result of negotiations between MIE and the OCR. "The amount reflects a negotiated settlement. It is possible that this is simply the amount that the parties agreed upon," explains Leeds.

HHS Posts New Fact Sheet on BAs' Liability

It's important that business associates (BAs) know what they're directly liable for and prepare, new federal guidance indicates.

The **Department of Health and Human Services Office for Civil Rights** (OCR) warns that covered entities (CEs) aren't the only ones who need to step up their HIPAA compliance. As more and more privacy and security issues arise, BAs also need to take ownership of their piece of the HIPAA violation puzzle.

To double down on BAs' role in care delivery and compliance, the OCR uploaded a new fact sheet to its online resources, outlining exactly what BAs are directly liable for. Specifically, the list of 10 requirements and prohibitions concern a BA's role in the failure to comply with the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules as well as the protections and limitations related to protected health information (PHI) disclosure.

"As part of the Department's effort to fully protect patients' health information and their rights under HIPAA, OCR has issued this important new fact sheet clearly explaining a business associate's liability," explains **Roger Severino,** OCR director, in an announcement on the new fact sheet. "We want to make it as easy as possible for regulated entities to understand, and comply with, their obligations under the law."

Resource: See the OCR fact sheet at www.hhs.gov/about/news/2019/05/24/new-hhs-fact-sheet-on-direct-liability-of-business-associates-under-hipaa.html.

Don't Let This Settlement Impact Your HIPAA Compliance

Even though the OCR's actions suggest a more lenient attitude, CEs and their various associates must continue to prioritize HIPAA compliance and funding. The MIE case does point to the problems that BAs have with following through on risk assessment, analysis, and management.

One expert warns not to confuse leniency with complacency. "I certainly do worry about compliance issues from an increasing perception that the risks of non-compliance are both remote and low," Kottkamp cautions. And he warns that if BAs assume an easy road, "we'll see a return to the pre-HITECH compliance attitude of many entities."

HHS Posts New Fact Sheet on BAs' Liability

It's important that business associates (BAs) know what they're directly liable for and prepare, new federal guidance indicates.

The **Department of Health and Human Services Office for Civil Rights** (OCR) warns that covered entities (CEs) aren't the only ones who need to step up their HIPAA compliance. As more and more privacy and security issues arise, BAs also need to take ownership of their piece of the HIPAA violation puzzle.

To double down on BAs' role in care delivery and compliance, the OCR uploaded a new fact sheet to its online resources, outlining exactly what BAs are directly liable for. Specifically, the list of 10 requirements and prohibitions concern a BA's role in the failure to comply with the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules as well as the

protections and limitations related to protected health information (PHI) disclosure.

"As part of the Department's effort to fully protect patients' health information and their rights under HIPAA, OCR has issued this important new fact sheet clearly explaining a business associate's liability," explains **Roger Severino,** OCR director, in an announcement on the new fact sheet. "We want to make it as easy as possible for regulated entities to understand, and comply with, their obligations under the law."

Resource: See the OCR fact sheet at www.hhs.gov/about/news/2019/05/24/new-hhs-fact-sheet-on-direct-liability-of-business-associates-under-hipaa.html.

Tip: Even though the MIE settlement leaves much room for interpretation, entities must continue to promote a compliant culture and follow the HIPAA Rules. "If OCR is imposing caps on liability based on factors, such as diligent effort, reasonable cause, and prompt correction, then entities subject to HIPAA should act in a way that allows them to argue that their liability is subject to those caps if they were ever to suffer a breach," advises Leeds.

Read the OCR release on the MIE settlement at www.hhs.gov/about/news/2019/05/23/indiana-medical-records-service-pays-100000-to-settle-hipaa-breach.html.