COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 23, Number 6. June 08, 2023 Five Years After 'a Singular Human Error,' Two Breach Notices, Revenue Firm Settles With OCR

By Theresa Defino

As far as settlements for alleged HIPAA violations go, a recent agreement announced by the HHS Office for Civil Rights (OCR) doesn't immediately jump out as particularly noteworthy. The amount paid by the practice management and IT firm—$350,000—is a far cry from the millions OCR used to command in such cases, and the number of patient records wasn't in the millions, either.

But most compliance officials know they should review all OCR's enforcement actions for insights. And when they dive into the agreement Matt Rolfes, president and CEO of MedEvolve Inc., signed with OCR in March, they'll discover a slightly more complicated story than just protected health information (PHI) left unguarded on a server for perhaps four months. The case demonstrates that—at least in the eyes of OCR—an organization can make an error when it concludes an incident isn't a breach.

The settlement documents reveal that OCR disagreed with MedEvolve's assessment of the number of records affected in June 2018 and required the Arkansas firm to make another public breach notification two years later.

"After five years, we are glad to have concluded the settlement," Rolfes said in an email in response to *RPP's* questions. "We look forward to moving beyond the incident with a bright future, creating new opportunities in healthcare, and helping healthcare organizations improve margin to further their missions."

MedEvolve's was the second settlement OCR announced in May. A Pittsburgh, therapist agreed to pay $15,000 as part of OCR's 44th records access initiative.[1]

MedEvolve, founded in 1998, provides revenue cycle management and other services. Under HIPAA, it is a business associate (BA), not a covered entity (CE). According to information MedEvolve released on July 10, 2018, the firm experienced a breach of PHI belonging to Premier Immediate Medical Care. At the time, MedEvolve said it "discovered that an FTP [file transfer protocol] containing a file with information related to certain Premier patients was inadvertently accessible to the internet."[2]

The firm's "investigation determined that the file was internet accessible from March 29, 2018, to May 4, 2018. The investigation also determined that one file was subject to unauthorized access on March 29, 2018," MedEvolve said. However, in its settlement documents, OCR listed a far longer period of public accessibility.

In its breach notification, MedEvolve did not disclose the number of individuals affected but said the PHI included "name, billing address, telephone number, the identification of patient's primary health insurer and the Social Security numbers for some of the individuals."

No "clinical information such as treatment or diagnosis or any financial information such as methods of payment" was exposed, it said. "The file was placed on the FTP server in question as part of an isolated data transfer event," MedEvolve said in 2018, adding the server was "not associated with MedEvolve's customer-facing 'front office.'" MedEvolve offered two years of credit monitoring services to those affected.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

"Upon discovery, MedEvolve immediately secured the portal in question and took steps to prevent further access," it said. "MedEvolve also hired a third-party forensic investigator to conduct an exhaustive investigation of this matter. As part of its ongoing commitment to the security of personal information in its care, MedEvolve [is] working to implement additional safeguards and security measures to enhance the privacy and security of information in its systems."

Proprietary Software Not a Safeguard

Fast-forward to Aug. 7, 2020. MedEvolve announced a "supplement" to the 2018 release—one it said was sparked by OCR.[3] "As a result of its cooperation" with OCR, MedEvolve provided breach notification to patients of a Corpus Christi, Texas, dermatologist. MedEvolve described Beverly Held, M.D., as a former customer.

Adding more details than in its 2018 release, MedEvolve said the file on the FTP server contained "an undecipherable combination of names, billing addresses, telephone numbers, primary health insurer and doctor's office account numbers and in some instances, Social Security numbers, relating to certain patients of Dr. Held."

After its investigation, MedEvolve "determined that although the file could have been accessed via the internet until May 4, 2018, the file was undecipherable without entering it into MedEvolve's proprietary software."

After conducting the breach notification analysis, MedEvolve determined "at that time, there was a low probability of compromise and risk to the data from Dr. Held's office due to the undecipherable nature of the file, which is why notification was not made earlier. However, in consultation and in compliance with recent instructions from [HHS], MedEvolve is providing notice at this time," it said in 2020. In this notification, as with the first, MedEvolve did not include the number of affected patients.

However, according to OCR, MedEvolve discovered that the server containing the PHI "had been unsecure and accessible on the internet since January 1, 2018."[4] The agency did not address when the information was secured. According to OCR, 204,607 of Premier's patients were affected, in addition to 25,965 of Held's, for a total of 230,572.

It is of interest that OCR—at least to date—has not pursued enforcement action against the CEs that had given MedEvolve their data. Experts advise that CEs have certain procedures in place to ensure BAs appropriately coordinate breach notification.[5]

What Subcontractor?

In addition to the $350,000 payment, MedEvolve agreed to implement a two-year corrective action plan (CAP), sanctions for what OCR said were three potential HIPAA violations—one of which is somewhat puzzling.

OCR alleged MedEvolve violated:

- 45 C.F.R. § 164.502(a), when it disclosed the PHI of the 230,572 individuals involved in a breach;
- 45 C.F.R. § 164.308(a)(1)(ii)(A), when it did not conduct a "sufficiently accurate or thorough" risk assessment of the "potential risks and vulnerabilities to the confidentiality, integrity, and availability of [electronic] ePHI held by it as a business"; and
- 45 C.F.R. § 164.502(e)(1)(ii), when it "failed to enter into a [BA] agreement with a subcontractor."

A subcontractor is mentioned only among the possible violations, and OCR provided no details about what sort of

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

entity this subcontractor was and whether it was involved in or responsible for the breach. Rolfes told *RPP* that no subcontractors were involved.

"The incident was the result of a singular human error and did not involve any third-party vendors," he said. "The cause of the incident was a data file that was inadvertently placed on [an FTP] server—separate from our client hosting environment—and had no impact on our technology solutions."

He added that, since the breach, "no malicious use of patient information has ever been detected. MedEvolve's application data was secure at the time of the incident and always has been."

The settlement amount, which Rolfes said was "determined by HHS," is likely lower than in the past because OCR reduced penalties during a successful challenge by the University of Texas MD Anderson Cancer Center, which refused to pay a $4.3 million fine.[6]

In addition to the payment amount, MedEvolve has been more fortunate than some that have run afoul of OCR. Since the breach, MedEvolve was not sued by any patients or part of class-action litigation that happens nearly universally after a breach. And it was not sanctioned by any state officials—something that happens fairly regularly, often occurring before OCR takes action.

Asked how he feels about the settlement, Rolfes said the firm "has been fully cooperative with HHS throughout its investigative process and remains steadfast in prioritizing the [CAP] agreed to with HHS as part of its settlement."

CAP Contains Common Requirements

The terms of the CAP require MedEvolve to first submit to OCR its plans for completing a risk analysis within 30 days of signing the agreement.

The analysis must cover the "security risks and vulnerabilities [and] incorporates all electronic equipment, data systems, programs and applications controlled, administered, owned, or shared by MedEvolve or its affiliates that are owned, controlled or managed by MedEvolve that contain, store, transmit or receive MedEvolve ePHI. As part of this process, MedEvolve shall include a complete inventory of all electronic equipment, data systems, off-site data storage facilities, and application that contain or store ePHI which will then be incorporated in its risk analysis."

In addition to the first one, MedEvolve must complete such an analysis yearly and "develop an enterprise-wide risk management plan to address and mitigate any security risks and vulnerabilities identified in the risk analysis."

The CAP also requires MedEvolve, more generally, to develop policies and procedures governing the privacy and security of PHI, submit them to OCR for approval and train its workforce on them. Training must occur annually for current employees and within 30 days of new workers beginning jobs that require them to access PHI.

As with other CAPs, MedEvolve officials must notify OCR of any policy or procedure violations within 60 days of any noncompliance and file an annual report during the two-year CAP summarizing its implementation as well as any reportable events.

Third-Party Certifications, Reviews Advised

Rolfes told *RPP* the firm's cyber insurance would cover the settlement amount. "Our cyber insurance provider has been very supportive of us and the process throughout," he said.

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.

RPP also asked if MedEvolve had made changes to its systems as a result of the breach. "Since the time of the incident, MedEvolve has implemented numerous additional security measures," he said. These include "utilizing a third-party to develop a remediation plan" and "significant investments in infrastructure," although Rolfes did not provide specifics.

MedEvolve also engaged in a "subsequent and ongoing" HIPAA compliance accreditation program, Rolfes said. "I do recommend obtaining third party compliance certifications and reviews to ensure a healthcare provider's business or its vendors are addressing all aspects of data security and compliance," he added.

"Data security is of utmost importance at MedEvolve, and we have made and continue to make significant investments since the 2018 incident to ensure our clients' data is protected and prevent future threats," Rolfes said.

1 Theresa Defino, "With Nearly Four Dozen Settlements, Records Access Mistakes Are Clear," *Report on Patient Privacy* 23, no. 5 (June 2023).
2 MedEvolve, "MedEvolve Provides Notice of Data Breach," news release, July 10, 2018, https://prn.to/30Dv7XK.
3 MedEvolve, "MedEvolve Expands Notification of Prior Data Security Incident," news release, August 7, 2020, https://bit.ly/430Qafu.
4 U.S. Department of Health & Human Services, "MedEvolve, Inc. Resolution Agreement and Corrective Action Plan," content last reviewed May 16, 2023, https://bit.ly/3NfIpmM.
5 Jane Anderson, "Security Checklist: Have These in Place Before a BA Breach," *Report on Patient Privacy* 23, no. 5 (June 2023).
6 Theresa Defino, "MD Anderson Won Against OCR, But Agency's Response—Including on Fines—Keeps Evolving," *Report on Patient Privacy* 22, no. 11 (November 2022), https://bit.ly/3qlAmvw.

This publication is only available to subscribers. To view all documents, please log in or purchase access.

Purchase Login

Copyright © 2024 by Society of Corporate Compliance and Ethics (SCCE) & Health Care Compliance Association (HCCA). No claim to original US Government works. All rights reserved. Usage is governed under this website's Terms of Use.