COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 7. July 10, 2019
On Heels of OCR's Reduction In Fines, Congress Offers Its Views

By Theresa Defino

In the roughly three months since the HHS Office for Civil Rights announced it planned to reduce the amount of fines imposed for all but the most serious HIPAA violations, OCR issued two settlements—but both were finalized before the change.

The health care privacy and security community, then, has yet to see how the recent decision by OCR Director Roger Severino plays out and, at the same time, what impact there might be on compliance.

Now Congress has entered the fray. Significant health care legislation is advancing in the Senate that calls for OCR, when dealing with HIPAA violators, to take into consideration whether a covered entity (CE) or business associate (BA) had "recognized security practices in place" for at least a year that would "mitigate fines" or "limit remedies" the agency might impose.

It could be argued that OCR already does this, but in recent years, particularly as its penalties have risen, the agency has stopped explaining how it arrived at settlement amounts. For example, last year OCR entered into a $16 million settlement with Anthem Inc. over a massive exposure of protected health information (PHI)—some 79 million records were involved. Severino said only that the "largest health data breach in U.S. history fully merits the largest HIPAA settlement in history" ("OCR Exacts Its Pound of Flesh From Anthem With $16 Million Settlement, Corrective Actions," *RPP* 18, no. 11).

Now Annual Caps Will Vary

Although specific decisions in individual settlements are not always disclosed, OCR's penalty structure since it implemented the 2009 HITECH Act has been based on four tiers with amounts assessed per violation and per year, with an annual cap for identical violations.

The tiers range from $100 per violation minimum for acts that an organization (defined as a person under the law) did not know "and by exercising reasonable diligence," would not have known, that the person violated a HIPAA provision to $500,000 for willful neglect and when the violation has not been corrected within 30 days.

Despite the differences, OCR has been applying a maximum of $1.5 million per year for all of the tiers, rather than at just the top or highest level of culpability.

It may be appropriate to thank the University of Texas MD Anderson Cancer Center for the reduction, as it came in the middle of a legal battle it is waging against a multimillion-dollar fine OCR has been trying to impose since 2017.

MD Anderson refused to settle and took its concerns to an HHS administrative law judge; in July 2018, OCR announced that the ALJ upheld the agency's intent to impose a fine of $4.358 million on MD Anderson for a stolen laptop and a USB drive lost in 2012 and $1.5 million for another drive reported missing in 2013. To this total OCR added $1.348 million for failing to implement access controls, specifically encryption and decryption ("Lack of Encryption Key to $4.3M Penalty For MD Anderson; 'Layered Security' One Solution," *RPP* 18, no. 7).

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.

This document is only available to subscribers. 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.