BUCK

US

FYI®
For Your Information®

Celebrating 40 years of FYI®

HIPAA Enforcement Reaches New Heights

Volume 42

Issue 37

April 17, 2019

Authors
Julia Zuckerman, JD
Amy Dunn, JD, MHA

In 2018 HHS's Office of Civil Rights collected $28,683,400 in HIPAA settlements and judgments. This sum includes the largest financial settlement OCR has ever reached with a covered entity — $16,000,000. Given the aggressive nature of current enforcement trends, it is increasingly important for covered entities to assess their HIPAA compliance efforts and address any related gaps.

Background

The Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) require covered entities (health care providers, health plans and health care clearing houses) to comply with privacy, security, and breach notification rules with respect to individuals' protected health information (PHI). (See our March 8, 2013 *For Your Information*.)

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces the HIPAA privacy, security, and breach notification rules. Every covered entity and business associate is eligible for an OCR HIPAA audit.

Civil monetary penalties range from $114 to $1,711,533, depending on the type, number, cause of the violation, and any corrective action taken (or not taken) to address it. In addition to civil monetary penalties, data breaches can result in costs relating to breach investigations, remediation, temporary operational changes, breach notification letters, identity theft protection, and reputational harm. Additionally, state attorneys general can bring civil actions to obtain damages on behalf of state residents for violations of the HIPAA Privacy and Security Rules.

2018 enforcement summary

OCR recently released a summary of its 2018 HIPAA settlements and judgments, which are up 347% since 2014. In total, OCR collected $28,683,400 in 2018. This included the largest financial

settlement OCR has ever reached with a covered entity — $16,000,000 against an insurance company in October 2018. Other large settlements included:

- $3,500,000 against a healthcare company in January 2018, involving "failure to conduct an accurate and thorough risk analysis of potential risks and vulnerabilities to the confidentiality integrity, and availability" of electronic PHI;
- $515,000 against a hospital in September 2018, where the hospital had brought in a film crew for a documentary series without first obtaining patient authorization; and
- $3,000,000 against a health system in December 2018, involving the failure to thoroughly and accurately assess, and address, risks to electronic PHI, and to obtain a written business associate agreement with a contractor that maintained PHI on the health system's behalf.

Additionally, OCR secured a $4,348,000 judgment against a cancer treatment center in June 2018 involving outdated electronic PHI encryption policies.

Critical considerations and action steps

Sponsors of self-insured group health plans should have the following in place:

- HIPAA privacy and security policies and procedures
- business associate agreements
- privacy notice
- documented risk analysis
- training materials
- security policies and procedures
- security risk analysis

These materials should be reviewed and updated periodically, and plans should be prepared to produce all of this documentation in the event of an audit.

Fully insured plans also have HIPAA obligations if they receive PHI. Additionally, sponsors of fully insured plans should be aware that if they self-insure any of their group health plan coverage — including a healthcare flexible spending account — HIPAA obligations apply.

Conducting an operational review can be an effective way to assess HIPAA compliance and identify any gaps that need to be addressed. This would entail a review of the administration of the plan, focusing on the plan's compliance with HIPAA privacy and security requirements.

Employers with on-site clinics, pharmacies and health centers should also be aware of HIPAA compliance requirements.

©2019 Buck Global, LLC. All rights reserved.

In closing

With OCR actively pursuing HIPAA enforcement, it is more critical now than ever for covered entities to assess — and address — HIPAA compliance risks.

Produced by the Knowledge Resource Center

The Knowledge Resource Center is responsible for national multi-practice compliance consulting, analysis and publications, government relations, research, surveys, training, and knowledge management. For more information, please contact your account executive.

You are welcome to distribute *FYI*® publications in their entireties. To manage your subscriptions, or to sign up to receive our mailings, visit our Subscription Center.

This publication is for information only and does not constitute legal advice; consult with legal, tax and other advisors before applying this information to your specific situation.

©2019 Buck Global, LLC. All rights reserved.