CARLTON FIELDS

2018 Was a Record Year in HIPAA Enforcement

HEALTH CARE | CYBERSECURITY AND PRIVACY | FEBRUARY 15, 2019

Megan K. Dhillon

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services recently announced that 2018 was a significant year in Health Insurance Portability and Accountability Act (HIPAA) enforcement activity. Last year, OCR received approximately $28.7 million in financial penalties – a record-breaker in terms of total penalty amounts paid, surpassing the $23.5 million OCR collected in 2016. OCR obtained the penalty amounts by settling 10 cases and receiving summary judgment in a case before an Administrative Law Judge.

2018 Enforcement Activity

OCR's announcement is particularly surprising, considering that many analysts initially thought enforcement activity would decrease in 2018. OCR had only entered into three settlements to resolve HIPAA violations by mid-year. But, enforcement activity picked up in the fall of 2018. In October, OCR issued the largest financial penalty ever imposed on a covered entity. Per the terms of the settlement agreement reached with the OCR, Anthem was required to pay $16 million and take substantial corrective action to resolve the HIPAA violations that led to the largest U.S. health data breach in history.

A common theme in OCR's enforcement activity in 2018 is that the majority of the enforcement actions involved entities that failed to conduct a thorough overview and assessment of potential security risks and vulnerabilities pertaining to maintaining and transmitting protected health information (PHI). Another commonality in the enforcement actions was that covered entities failed to obtain written business associate agreements with contractors and other entities prior to transmitting PHI. OCR's 2018 enforcement actions and the costly financial settlements imposed indicate that covered entities need to be proactive about data security.

How to Ensure HIPAA Compliance

OCR has made it clear that there will be no slowdown in its enforcement activities. Therefore, health care organizations must be cognizant about achieving HIPAA compliance and should take steps to secure and protect patient privacy information. The following are some steps organizations can take to ensure HIPAA compliance and help prevent being the subject of an OCR enforcement action:

Perform a Security Risk Analysis

Pursuant to 45 C.F.R. § 164.308, a covered entity is required to conduct an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information." Yet, many organizations do not adequately or routinely assess the risks associated with maintaining and transmitting PHI. To conduct a thorough risk assessment, covered entities should:

- Identify the PHI the organization creates, receives, stores, and transmits, including PHI shared with business associates and other contractors;
- Identify the threats and vulnerabilities to the integrity of the PHI, including both intentional and negligent human actions;
- Determine the various probabilities of a PHI breach occurring and evaluate the likely impact of a breach;
- Evaluate the measures in place to protect against the identified threats; and
- Consider what procedures, security measures, and policies are necessary to safeguard against a PHI breach.

Covered entities should thoroughly document the results of a risk assessment and maintain the documentation for at least six

years. In addition, covered entities should review the results of the risk assessment annually to reassess whether current safeguards are sufficient to protect against vulnerabilities and threats to PHI. Conducting and documenting the results of a risk assessment is the most useful method to prevent HIPAA violations from occurring, and to mitigate the imposition of any financial penalty should a violation occur.

Execute a Business Associate Agreement Prior to Disseminating PHI

The OCR has determined that transmitting and sharing PHI without the presence of a business associate agreement (BAA) is grounds for a HIPAA violation and imposition of a financial penalty. Covered entities need to track arrangements carefully with outside vendors or contractors. Prior to sharing PHI, covered entities must ensure that a BAA is executed. The BAA should clearly specify the permitted uses and disclosures of PHI and how PHI should be returned or safeguarded upon the termination of the agreement.

Equally important, covered entities should monitor access to PHI following the termination of its contractual agreement with outside vendors, consultants, or employees. In November 2018, OCR reached a settlement with Pagosa Springs Medical Center, which allowed a former employee to maintain remote access to a scheduling calendar that contained PHI. Upon the termination of a contractual agreement, covered entities must confirm any PHI shared under a BAA is returned or appropriately safeguarded by the business associate. In addition, covered entities must ensure that former employees, contractors, or business associates do not maintain access to PHI, at least not without a BAA.