Health Information Compliance Alert

Case Study: OCR Pushes HIPAA Enforcement to New Heights in 2018

Hint: Breaches drew huge penalties for risk assessment fails.

If your office budget doesn't include money put aside for risk planning and management, you may want to revisit your financial outlays. HIPAA enforcement activity in 2018 shows that the feds mean business and will not hesitate to punish negligent organizations severely.

Background: Last year, the **HHS Office for Civil Rights** (OCR) steamrolled past its previous enforcement record - big time. "In 2018, OCR settled 10 cases and was granted summary judgment in a case before an Administrative Law Judge [ALJ], together totaling $28.7 million from enforcement actions. This total surpassed the previous record of $23.5 million from 2016 by 22 percent," announced OCR in a release. The OCR's $16 million settlement with **Anthem, Inc.** was the single largest HIPAA settlement ever, tripling the previous leader at $5.5 million in 2016, noted the agency.

The significant enforcement was unexpected as trends suggested activity was declining. "OCR's announcement is particularly surprising, considering that many analysts initially thought enforcement activity would decrease in 2018," writes Washington, D.C.-based attorney **Megan K. Dhillon** of national law firm **Carleton Fields** in online legal analysis.

Plus, "OCR had only entered into three settlements to resolve HIPAA violations by mid-year," Dhillon says. But by fall, OCR was on a roll that included the monster settlement with Anthem in October, Dhillon indicates.

Finale: The agency ended 2018 with a $3 million settlement with **Cottage Health,** which operates four hospitals in California. The organization's failure to fully assess risks and follow through on security measures and management led to breaches in 2013 and 2015 that exposed 62,500 individuals' electronic protected health information (ePHI), the OCR release said.

What Sparked the Enforcement Upswing?

A number of variables impacted the OCR's uptick in enforcement activities this past fall, experts say. OCR locked up open breach cases, finalizing settlements and agreements. The agency heightened its scrutiny of Privacy and Security Rule basics, too, shining a spotlight on the continued problem many organizations have with updating and maintaining HIPAA protocols.

"I think there are multiple factors leading to escalating enforcement. The short answer is: enforcement is escalating because enforcement is escalating," says **Adam Kehler, CISSP,** principal consultant and healthcare practice lead with **Online Business Systems**. "This means that OCR continues to increase its efforts in investigating breaches and compliance efforts. The natural result is that fines are increasing."

Timeline: Kehler adds, "Also, we are just starting to see settlement agreements come out for breaches that occurred 5-plus years ago. While 2018 was a banner year for enforcement actions, you will note from the Cottage Health settlement agreement, the breaches actually occurred in 2013 and 2015."

Lax protocols: OCR reveals that the lack of data-security implementations is a big part of the hefty enforcements. "Our record year underscores the need for covered entities [CEs] to be proactive about data security if they want to avoid being on the wrong end of an enforcement action," said OCR Director **Roger Severino**.

In fact, a "common theme" emerged in 2018, Dhillon suggests. The settlements show that many CEs lacked business associate agreements (BAAs) with their partners and vendors to their own demise, she indicates. In addition, "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],"

she maintains.

Speed of Health IT Threats Impedes HIPAA Success

Though HIPAA has been around for quite a while, technology has thrown a wrench into compliance. Caring for patients is a provider's primary concern, and health IT helps make that pursuit more efficient. However, health IT tools are constantly evolving, multiplying, and becoming more sophisticated - and the healthcare industry continues to struggle to keep up with new programs, better upgrades, and the density of patients' data.

This data and program overload exacerbates the breach problem, and definitely added to the OCR's enforcement tour-de-force last year. Moreover, "the sheer volume of data and number of systems in healthcare are increasing, thereby increasing the attack surface," warns Kehler.

"Practices - especially small-to-midsize practices - don't have the resources or expertise to dedicate to information security. As we see with other industries, adoption comes first followed by security," Kehler explains. "I would say that we are near the end of the adoption phase and many in the industry are just starting to realize the time, effort, and money that should be dedicated to security as a result."

Best bet: It's not enough to write up a HIPAA compliance plan and have it sitting on your shelf. You must manage it and implement safeguards to cut down your chances of a breach. And more importantly, make it part of your practice culture, ensuring every employee is committed to doing the right thing when it comes to HIPAA security.

Resource: Read the OCR release at www.hhs.gov/about/news/2019/02/07/ocr-concludes-all-time-record-year-for-hipaa-enforcement-with-3-million-cottage-health-settlement.html.