Codify
BY AAPC

Health Information Compliance Alert

HIPAA Enforcement: Feds Keep Pressure on Despite PHE

Tip: Make risk management a priority in 2021.

You might think that a pandemic would impede HIPAA enforcement, but you'd be wrong. In fact, as COVID-19 hits its third-wave stride, the feds seem to be trending up rather than down.

Backtrack: Through the spring, the **HHS Office for Civil Rights** (OCR) released a steady stream of notices of enforcement discretion in light of the COVID-19 public health emergency (PHE). These flexibilities and waivers were to deal with HIPAA compliance as it relates to COVID-19-specific issues and to thwart the spread of the virus. However, due to the chaos and uncertainty caused by the pandemic, many believed that the agency might ease up on its HIPAA enforcement in other areas, too, during the PHE.

This has not been the case. In reality, OCR has remained extremely prolific, levying one settlement after another in one of its busiest years in a while.

Register 3 Security Violation Settlements

OCR settled a cornucopia of hacking cases this fall, resulting in million-dollar breach price tags for the organizations. Over the last few years, data security incidents have garnered the biggest settlements, costing covered entities (CEs) big bucks.

"Hacking is the number one source of large healthcare data breaches. Healthcare providers that fail to follow the HIPAA Security Rule make their patients' health data a tempting target for hackers," said OCR Director **Roger Severino** in a release on one of the cases.

Here's a breakdown of the three major settlements:

1. Provider: Back in June 2016, a journalist alerted Georgia-based **Athens Orthopedic Clinic PA** that 208,557 patients' protected health information (PHI) was listed online for sale. After the hackers demanded money for the database, Athens Orthopedic determined that the cyber thugs had usurped their vendor's credentials. It took the organization another month to finally let OCR know about the breach.

After a thorough investigation, the agency uncovered years of "systemic noncompliance" with the HIPAA rules, including risk analysis failures, poor workforce training and audit controls, and less than stellar business associate (BA) agreements, an OCR release indicates. In September, Athens Orthopedic agreed to pay $1,500,000 to settle the breach and also enter into a "robust" two-year corrective action plan (CAP) with OCR monitoring.

Note the Athens Orthopedic details at www.hhs.gov/about/ news/2020/09/21/orthopedic-clinic-pays-1.5-million-to-settle-systemic-noncompliance-with-hipaa-rules.html.

2. Business Associate: In 2014, the **Federal Bureau of Investigation** (FBI) let Franklin, Tennessee-based **CHSPSC LLC** know "that it had traced a cyberhacking group's advanced persistent threat to CHSPSC's information system," notes an OCR release. Eventually, CHSPSC, an IT and health management firm that offers BA services to hospitals and physicians, discovered that administrator credentials had been compromised, and hackers had accessed 6,121,158 individuals' PHI through a virtual private network (VPN).

CHSPSC's problems run the gamut of HIPAA security fails from risk analysis and access issues to monitoring and logging problems. In September, the firm agreed to a $2.3 million settlement with OCR and a two-year CAP with monitoring.

Sift through CHSPSC's case at www.hhs.gov/about/ news/2020/09/23/hipaa-business-associate-pays-2.3-million-settle-breach.html.

3. Private Payer: Insurance giant **Premera Blue Cross** (PBC) conceded to pay OCR $6.85 million to settle a breach caused by a cyber attack back in 2014; a two-year CAP with OCR monitoring was also mandated. For over nine months, the hackers harvested patients' data undetected in an "advanced persistent threat," says a release. More than 10.4 million individuals' PHI was exposed, from birth dates to emails to Social Security numbers and more.

An OCR probe into the organization's HIPAA compliance revealed a plethora of longstanding security problems. PBC failed "to conduct an enterprise-wide risk analysis, and failures to implement risk management, and audit controls," the agency says.

Find the PBC settlement and CAP at www.hhs.gov/about/ news/2020/09/25/health-insurer-pays-6-85-million-settle-data-breach-affecting-over-10-4-million-people.html.

Other Cases Touch on HIPAA Privacy and Inside Threats

Despite the rise in digital violations, HIPAA privacy incidents still occur. "Something as simple as a letter shifting inside an envelope, or the failure to confiscate an office key from a terminated employee, can contribute to the impermissible disclosure of PHI," remind attorneys **Erin Doyle** and **Madison Poole** with law firm **Arnall, Golden, Gregory LLP** in online analysis.

HIPAA hat trick: One organization had both a privacy and security breach - and a third incident to round out the trio. In October, **Aetna Life Insurance Company**, which operates in the U.S. as a managed healthcare company offering traditional and consumer-directed health insurance, agreed to a $1 million settlement from OCR and a two-year CAP for three separate HIPAA breaches. The violations include the following:

- In 2017, Aetna's web services were breached and allowed access to health plan data without login credentials, a brief states. The PHI of 5,002 individuals was impacted.
- During the same year, the organization sent out window envelopes to members that exposed sensitive information concerning HIV medication. The impermissible disclosure was a HIPAA privacy violation affecting 11,887 people.
- Aetna had another mailing snafu in late 2017. It sent letters to plan members involved in an atrial fibrillation research study that listed the information on the outside of the envelope, exposing the PHI of 1,600 folks.Inquiries into Aetna's practices showed the organization had a laundry list of HIPAA fails across the administrative, technical, and physical safeguards spectrum, an OCR release suggests.

See the Aetna case specifics at www.hhs.gov/about/ news/2020/10/28/aetna-pays-one-million-to-settle-three-hipaa-breaches.html.

Staff mix-up: In 2016, the **New Haven Health Department** in Connecticut forgot to cut a former employee's access to both the facility and the computer after termination. The staff member re-entered the job site eight days after leaving and used her login and password to steal the PHI of 498 patients. "Additionally, OCR found that the former employee had shared her user ID and password with an intern, who continued to use these login credentials to access PHI on New Haven's network after the employee was terminated," a release says.

Similar to the other settlements, New Haven agreed to a two-year CAP and OCR monitoring; the organization will also pay the feds $202,400 to settle the violations.

Review the New Haven facts and resolution at www.hhs.gov/ about/news/2020/10/30/city-health-department-failed-terminate-former-employees-access-protected-health-information.html.

Bottom line: "Covered entities must consider all methods in which they maintain, transfer, and protect PHI to ensure it is kept secure and only disclosed to intended recipients," Doyle and Poole caution.