Health Information Compliance Alert

Case Study: Get a Grip on HIPAA Security

Tip: Encrypt devices or pay the price.

Whether your organization is big or small, it's critical to have a handle on the requirements of the HIPAA Security Rule. And with a majority of states' COVID-19 rates peaking, more providers will be conducting business online or communicating with patients via mobile devices - and that means more opportunity for potential violations.

Register 2 Recent Settlements

Though the **HHS Office for Civil Rights** (OCR) has been relatively quiet on the enforcement front in 2020, violations have continued to escalate. According to the OCR breach portal, there have been 268 breaches this year as of August 7. More than 230 of the incidents fall under the HIPAA Security Rule jurisdiction and point to IT issues, hacking, impermissible disclosure, unauthorized access, and email snafus.

In July, two organizations agreed to resolve Security Rule issues with settlements and corrective action plans (CAPs). Here's a breakdown of the cases:

1. Metropolitan Community Health Services (Metro): Operating as a Federally Qualified Health Center (FQHC) in North Carolina, Metro provides medical and dental services to an underserved population. On July 23, OCR announced that Metro, doing business as **Agape Health Services**, would pay the feds $25,000 to settle potential HIPAA violations. In addition, the rurally based, small organization also agreed to adopt a CAP that includes two years of OCR monitoring.

During an investigation of a June 9, 2011 breach, OCR discovered that Metro had a history of "longstanding, systemic noncompliance with the HIPAA Security Rule," an impermissible disclosure of PHI to an unknown email account, impacting 1,263 patients.

"Healthcare providers owe it to their patients to comply with the HIPAA Rules," said OCR Director **Roger Severino** in a release on the Metro case. "When informed of potential HIPAA violations, providers owe it to their patients to quickly address problem areas to safeguard individuals' health information."

Tip: Covered entities (CEs) can learn a lot from this settlement, particularly smaller providers, suggests attorney **Linn F. Freedman** with **Robinson & Cole LLP** in the law firm's Data Privacy & Security Insider blog. "As with all settlements that the OCR enters into with regulated entities, lessons can be learned from this one, including consideration of reviewing the last time a security risk assessment was performed, review of a business' HIPAA compliance program, including policies and procedures that comply with the Security Rule, and security awareness training for its workforce," Freedman advises.

View the details of the Metro settlement at www.hhs.gov/about/news/2020/07/23/small-health-care-provider-fails-to-implement-multiple-hipaa-security-rule-requirements.html.

2. Lifespan Health System Affiliated Covered Entity (Lifespan ACE): The Rhode Island-based Lifespan ACE, which is a nonprofit health system, consented to two years of OCR monitoring and a CAP to rectify the loss of an unencrypted laptop that affected 20,431 individuals' electronic PHI (ePHI). Lifespan ACE's monetary settlement was quite a bit bigger than the other case at a whopping $1.04 million to settle the breach.

Plus, while looking into Lifespan ACE's violation and security practices, OCR unearthed a history of noncompliance with the HIPAA Rules, including "a lack of device and media controls, and a failure to have a business associate agreement [BAA] in place with the **Lifespan Corporation**," an agency release related. One of the major factors leading to its large settlement was not encrypting laptops after being instructed to do so, OCR indicated.

"Laptops, cellphones, and other mobile devices are stolen every day, that's the hard reality. Covered entities can best protect their patients' data by encrypting mobile devices to thwart identity thieves," said Severino.

"Together with the Metro resolution agreement, these settlements illustrate OCR's continued and longstanding emphasis on Security Rule requirements and underscore that compliance is critical for all providers, large and small," warn attorneys **Erin Doyle** and **Madison Poole** with **Arnall, Golden, Gregory LLP** in online analysis.

Read the resolution details at
www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html.

Reminder: OCR has moved slowly in 2020, most likely due to the onset of COVID-19 and other more pressing policy concerns. Metro and Lifespan ACE are only the second and third settlements of the year. The first case resolved a Security Rule issue related to a CE's business associate (BA) (see Health Information Compliance Alert, Vol. 20, No.3).

Ask Yourself These 5 Questions

All three of the 2020 settlements have two things in common. First, the organizations failed to remedy longstanding security issues. Second, when the CEs ignored the requirements of the HIPAA Rules, they neglected to safeguard their patients' PHI and ePHI.

With HIPAA enforcement expected to increase in the months ahead, you may want to revisit your protocols, assess and analyze your risks, and manage the outcomes. Consider asking yourself these five questions as you go about outlining your policies and procedures:

1. Does my current HIPAA plan resonate with industry trends and cover the needs of my business now?
2. Are my BAs and vendors aware of recent OCR updates, policy changes, and IT requirements and are they in line with the plethora of COVID-19-related rollbacks, too?
3. Is my organization's IT team on top of the latest security trends and tools, including cybersecurity basics like patch management, mobile device management, encryption, password protection, multifactor authentication, pentests, and more?
4. Does my organization promote a culture of compliance and mandate HIPAA training for all staff with frequent refresher courses?
5. Are all my disclosures, notifications, releases, contracts, and agreements up to date and in accord with the necessary HIPAA requirements?

Resource: Check out OCR guidance on the HIPAA Rules, risk analysis, planning, and more at www.hhs.gov/hipaa/for-professionals/index.html.