So far 2017 is proving to be an active year for Health Insurance Portability and Accountability Act (HIPAA) enforcement. This comes on the heels of 2016, which saw an unprecedented level of enforcement actions, with 13 total settlements and nearly a 300 percent increase in total collected fines over 2015. To date in 2017, nine actions have been settled and the average settlement amount continues to outpace 2016.

Three Tips to Help Reduce the Risk of a HIPAA Violation

Several themes have emerged from these enforcement actions that HIPAA-regulated
entities should be mindful of to help reduce the risk of a HIPAA violation occurring and to reduce the potential resulting fine in the event of enforcement.

1. **Conduct Risk Analyses Regularly.** One of the most consistent themes that has emerged from the 2017 settlement and corrective action plans announced by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) is that organizations subject to HIPAA must regularly conduct risk analyses in accordance with the Security Rule to assess risk and vulnerabilities in an organization’s ePHI environment. The Security Rule does not proscribe a specific risk analysis methodology given that the analysis will vary depending on an organization’s size and capabilities. However, the risk analysis should comply with available OCR guidance, including the [Guidance on Risk Analysis Requirements under the HIPAA Security Rule](https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html).

   > [A] lack of risk management not only costs individuals the security of their data, but it can also cost covered entities a sizable fine.
   > – OCR Acting Director Robinsue Frohboese

2. **Implement a Risk Management Plan and Reasonable Safeguards.** While conducting a risk analysis is critical, equally important is the risk management plan and the reasonable safeguards an organization adopts in light of any risks or vulnerabilities that are identified in the risk analysis. For example, OCR assessed a $3.2 million civil monetary penalty against a hospital in February, after noting that the hospital continued to use unencrypted devices even after reporting a breach in 2009 involving the loss of an unencrypted, non-password protected device. Note that the issuance of a penalty is rare, as most OCR enforcement actions result in a settlement, not a penalty. Here, however, the hospital chose to pay the penalty as opposed to negotiate with OCR.

3. **Report Breaches in Timely Manner.** A settlement announced in January made headlines as the first HIPAA settlement based on the untimely reporting or notification of a breach under the HIPAA Breach Notification Rule. OCR found that the healthcare network failed, with unreasonable delay, to notify OCR, the affected individuals, and the media within the required 60-day timeframe. Instead, the notifications were made over 100 days after discovery of the breach. This settlement highlights the importance of having clear policies and procedures that workforce members have been trained on in order to respond within HIPAA’s breach notification timeframes.

**OCR Updated Web Tool**

OCR recently announced the release of an [updated web tool](https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html) to provide enhanced transparency to the HIPAA breach reporting tool. New features include: 1) breaches
currently under investigation and reported within the last 24 months; 2) an archive of all older data breaches; 3) tips for consumers; and 4) navigation to additional breach information.

© 2020 Foley & Lardner LLP