COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 9. September 30, 2018 $115M Settlement Ties Anthem to Security Upgrades, Certain Staffing, Spending Levels

By HCCA Staff

Among the 31 FAQs the administrator of the new $115 million Anthem Inc. settlement posted on the website for filing claims is the following: "Will the Settlement help protect data stored by Anthem from another data breach?"

Odds are the estimated 80 million Anthem members and former enrollees affected by the breach are more likely to wonder how much of the $115 million they might receive. Spoiler: $50, or several years of credit monitoring and $10,000 in credit remediation, if required.

However, this provocative question is probably top-of-mind for Anthem officials, already chastened by being party to the most expensive data breach settlement in history, and for HIPAA compliance officials at other health plans, hospitals and provider organizations that don't want to end up like Anthem.

But they can learn from the experiences of the nation's second largest insurer. As with a typical HIPAA state or federal settlement with the HHS Office for Civil Rights (OCR), Anthem's class action suit resolution carries with it requirements to shore up the security of its data. These are spelled out in a list of 13 "business practices," but 11 of these are fully or partially redacted.

Still, the Anthem deal, approved Aug. 17, holds some gems in this regard—the plan is required, for example, to triple the amount it was spending on "information security" when the hacking occurred in 2014-2015, and maintain that level for three years.

In addition, the settlement obligates Anthem to boost future spending as membership increases, and it must provide security reports to the plaintiffs' attorneys for their review.

The world learned of the breach in February 2015 (*RPP 3/15, p. 1*).

But according to a report issued with an earlier Anthem settlement with state insurance commissioners, the breach "began on February 18, 2014, when a user in Anthem's Amerigroup subsidiary opened an e-mail (commonly referred to as a 'phishing' e-mail) containing malicious content. Opening this e-mail permitted the download of malicious files to the user's local system, allowing the Attacker to gain remote access to that computer. Starting with the initial remote access, the Attacker was able to move laterally (across Anthem systems) and escalate privileges (gain increasingly greater ability to access information and make changes in Anthem's environment). The Attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the Company's enterprise data warehouse—a system that stores a large amount of consumer personally identifiable information ('PII'). Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 million unique user records."