Home Medical Equipment Provider Attacked by Ransomware

More than 500,000 patients' data may have been compromised.

In late June, Airway Oxygen, based in Michigan, reported to the U.S. Department of Health & Human Services (HHS) that its system had been accessed by intruders, who installed ransomware that locked employees out. Although the company says there is no indication, at this point, that patient data was accessed, protected health information (PHI) was stored on the network and, therefore, is considered compromised.

"An investigation revealed that the intruders had access to patient health information for approximately 550,000 current and past customers of Airway Oxygen. Additionally, the personal information of approximately 1,160 current and former employees of Airway and its sister company were also compromised," BankInfoSecurity reported.

In a letter sent to customers, Airway Oxygen attempted to assure them that such incidents wouldn't occur again. "Since learning of the incident, we immediately took steps to secure our internal systems against further intrusion, including scanning the entire internal system, changing passwords for users, vendor accounts and applications, conducting a firewall review, updating and deploying security tools, and installing software to monitor and issue alerts as to suspicious firewall log activity." The letter also states that Airway Oxygen hired a cyber-security firm to help investigate the "cause and impact of the breach."

While news of these types of ransomware attacks is becoming more common, organizations continue to be unprepared and are paying the price. In addition to whatever money may have been paid in "ransom" (which was not disclosed) plus the time and money spent after the fact to prevent future incidents, Airway Oxygen may face serious penalties for HIPAA violations. According to the HHS publication, "FACT SHEET: Ransomware and HIPAA," when electronic PHI (ePHI) is "encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA Privacy Rule."

For all these reasons, it’s wise to address your security issues before they become serious problems. There will be some up-front costs, but those pale in comparison to what organizations such as Airway Oxygen are likely to pay after breaches occur.

Protect your HME/DME or other home care business with CareTend hosted by Mediware. Our secure data center ensures that your patients’ PHI is protected by the tightest security standards in the healthcare industry. Learn more at www.mediware.com.