Report on Patient Privacy Volume 19, Number 2. February 28, 2019 SingHealth Breach Caused by Vulnerability in Code; Case Holds Key Lessons for U.S. Entities

By Jane Anderson

A massive data breach in Singapore, which released medical information for around 1.5 million individuals covered by SingHealth, ultimately was caused by inadequate cybersecurity training and was exacerbated by poor management and existing vulnerabilities in the system.

That's the word from a report released in January dissecting the breach, which holds lessons for HIPAA covered entities and business associates in the United States. "These imperatives apply equally to all organizations responsible for large databases of personal data," said the 454-page report, issued by the Singapore Committee of Inquiry formed to investigate the breach. "We must recognize that cybersecurity threats are here to stay, and will increase in sophistication, intensity and scale."

David Harlow, principal in health care law at consulting firm The Harlow Group LLC, says the report echoes the cybersecurity problems faced by U.S. health care entities. "All of the major cases of the past year or so relate to these sorts of issues," Harlow tells *RPP*. "These sorts of recommendations need to be taken to heart by health care organizations everywhere."

Among the key events that led to the breach and potentially made it worse:

- A now-fired employee discovered a coding vulnerability in Allscripts Healthcare Solutions Inc.'s Sunrise electronic health record (EHR), which was in use at SingHealth, but elected to disclose the vulnerability to Epic Systems Corporation instead. The vulnerability ultimately led to the attack.
- SingHealth's information technology administrators noticed suspicious activity over a period of almost a month, but didn't realize that it might mean a serious cyberattack was underway.
- Key IT management personnel at SingHealth failed to take action in a timely and effective manner, in part because they were afraid of a false alarm.

The SingHealth cyberattack occurred between Aug. 23, 2017, and July 20, 2018. Personal data from almost 1.5 million SingHealth patients, including names, identification numbers, addresses, genders, races and dates of birth, were exfiltrated between June 27 and July 4, 2018. Around 159,000 of those nearly 1.5 million patients also had their outpatient dispensed medication records stolen. Prime Minister Lee Hsien Loong's personal and outpatient medication data "was specifically targeted and repeatedly accessed," according to the report.