

Report on Patient Privacy Volume 18, Number 6. June 30, 2018 Privacy Briefs: June 2018

By HCCA Staff

◆ LifeBridge Health, Inc., has notified half-a-million patients that their personal information may have been exposed in a cyber attack dating from September 2016. The Baltimore-based health system first detected the breach in March, and a forensic firm determined when the breach first took place. The attacker accessed the health system's servers through one of its physician practices, LifeBridge Potomac Professionals. Information that may have been taken includes names, addresses, birth dates, insurance information and Social Security numbers from the patient registration and billing system. The health system says it doesn't believe anyone's information was misused, but says it is offering credit monitoring to patients whose Social Security numbers were included in the breach. Read more about the breach at <https://bsun.md/2IEO6qw>.

◆ A software start-up company that provides independent insurance brokers with customer management software has exposed protected health information and financial data on thousands of insurance policy holders. The cache of data was stored on an Amazon S3 storage bucket by AgentRun, a Chicago-based company founded in 2012 by a former independent insurance broker. The bucket stored thousands of files of broker clients, which included insurance policy documents, health and medical information, and some financial data. The bucket wasn't protected with a password and was accessible to anyone. Andrew Lech, the company's founder, admitted the breach. Read more at <https://zd.net/2GMdusz>.

This document is only available to subscribers. Please log in or purchase access.

[Purchase Login](#)