More Accellion Health Data Breaches Revealed

By Marianne Kolbasuk McGee

Archived: 2026-04-05 20:29:02 UTC

3rd Party Risk Management , Data Breach Notification , Governance & Risk Management

Four More Health Plans Report They, Too, Were Affected (HealthInfoSec) • April 6, 2021

This article has been updated.

See Also: Live Hacking into Microsoft 365

Months after the December cyberattack on Accellion's File Transfer Appliance, the identities of more healthcare sector entities that were affected continue to come to light.

In the last few days, the Department of Health and Human Service's HIPAA Breach Reporting Tool website has added several large breaches tied to attacks on unpatched Accellion FTA installations.

Among the latest victims added are health plans that are owned by Centene Corp., which recently filed a lawsuit against Accellion in the wake of the incident. Those health plans are:

- Health Net Community Solutions, with nearly 687,000 individuals affected;
- Health Net of California, with 524,000 individuals affected;
- California Health & Wellness, with 80,000 affected;
- Health Net Life Insurance Co., with nearly 27,000 affected.

Other Victims

Other organizations that have revealed in recent weeks that they were victims of the Accellion breach include Trinity Health, Stanford University School of Medicine, the University of California, and UC Davis.

Earlier, supermarket chain Kroger, Springfield, Illinois-based Southern Illinois University School of Medicine; Trillium Community Health Plan based in Springfield, Oregon; and Canada-based Nova Scotia Health Employees' Pension Plan also confirmed they were victims.

Third-Party Risks

"New types of cyberattacks targeting service providers have dramatically increased the risk of compromise to health information impacting large segments of the industry," says privacy attorney David Holtzman of the consulting firm HITprivacy LLC.

"Growing public awareness of new cybersecurity threats like ransomware along with increased government oversight is throwing sunlight on the pervasive vulnerabilities plaguing the infrastructure that supports healthcare's information ecosystem."

An Accellion spokesman tells Information Security Media Group that the company is not breaking out by industry those customers affected by the FTA breach. But it says fewer than 100 of approximately 300 FTA users were affected. "Within this group, fewer than 25 appear to have suffered significant data theft," he notes.

"The Accellion breach is unique from many others in that it represents a data compromise exposure by a company that specializes in the file sharing and collaboration - as compared to, for instance, Blackbaud's primary work as a processor of payment or other transaction processing data," says Jim Van Dyke, senior vice president of financial wellness at security vendor Sontiq.

A 2020 attack on Blackbaud exposed the PHI of more than 11 million individuals.

Trinity Health was affected by both the Accellion and Blackbaud incidents. Last September, Trinity Health notified 3.3 million individuals that their PHI was potentially compromised in the Blackbaud incident. Trinity Health's Accellion-related breach, added to the HHS OCR website on Wednesday, indicates nearly 587,000 individuals are affected this time.

Fraud Threat

In the Accellion incident, attackers used reverse engineering to drop a web shell - a script that enables remote execution of commands - onto servers running the unpatched FTA software, according to FireEye's Mandiant incident response group, which Accellion hired to investigate (see: *Accellion Attack Involved Extensive Reverse Engineering*).

The web shell allowed attackers to bypass authentication, remotely execute code on the vulnerable systems and steal data, Mandiant says. In at least some cases, stolen data ended up in the hands of the Clop ransomware gang, which has been offering to sell it or to remove it if victims pay a ransom, some clients report (see: *Accellion: How Attackers Stole Data and Ransomed Companies*).

What's important about the Accellion breach is that "because the exposure was of a file-sharing organization, all manner of personal data may have been exposed," Van Dyke notes. In some cases, that includes "Social Security numbers and other data ideal for committing the worst kinds of identity theft, such as new financial account fraud, tax refund fraud," he points out. And because several healthcare organizations had medical data exposed as well, that raises the risk of medical identity theft, he adds.

Ongoing Challenges

Attacks on third-party providers "highlight the failure to uphold the chain of trust to safeguard an information ecosystem that relies on industry self-regulation, contractual agreements and limited enforcement of government regulatory standards," Holtzman says.

He calls for the creation of a common standard for cybersecurity that all organizations involved in the information ecosystem must meet, universal requirements for proof of testing and risk assessment, and meaningful enforcement carried out by a government-backed entity.

"While this will not be a quick solution, the threat will not diminish until there is a comprehensive, mandatory framework of standards that apply to all," he adds.
