# Bond Case Briefs

*Municipal Finance Law Since 1971*

---

## Fitch: Recent Cyberattacks Highlight Credit Risk to Vulnerable NFP Hospitals

Fitch Ratings-San Francisco/New York/Austin-19 March 2025: Recent cyberattacks on U.S. not-fo--profit (NFP) hospitals have highlighted the risk to some healthcare providers, particularly smaller hospitals or hospitals with fewer financial resources, Fitch Ratings says.

Threat actors continue to target hospitals and health systems given the sensitive data they maintain and technology vulnerabilities, including use of third-party vendors and equipment. While most cyber events to date have not materially affected a hospital's credit quality, Fitch recently took rating actions on two healthcare credits, Frederick Health Hospital in Maryland and Palomar Health in California, partly because of cyber incidents. Both providers are comparatively smaller with relatively weaker balance sheets and limited cushion for additional stress when compared to Fitch's rated universe.

On March 14, 2025, Fitch downgraded Palomar's Issuer Default Rating (IDR) to 'B-'/RON from 'B'/RWN due to continued financial challenges. This follows a downgrade in December 2024 from 'BB+'/RON due to pressured financial performance, which was exacerbated by a significant cyber event whose recovery lasted several months and severely disrupted operations and key billing functions.

Fitch downgraded Frederick Health's IDR to 'BBB'/RWN from 'BBB+' in February 2025 as a result of slower-than-expected recovery in operating performance. However, the RWN reflects uncertainty around the financial and/or reputational impact a recent cyberattack will have on the hospital. Fitch believes the attack and potentially prolonged recovery may lead to a heightened level of stress and weaken financial metrics.

These rating actions underscore the importance of robust cyber resilience measures to withstand and quickly recover from cyber incidents, although issuers with fewer resources may have a more difficulty improving current cyber defenses.

Fitch may take negative rating action if a hospital's financial profile is deemed to be materially impaired, or at risk for impairment, in the aftermath of a cyber event. A cyberattack that affects a hospital's ability to provide service, including affecting relationships with physicians and staff, and/or hinders customer billing could temporarily reduce revenue generation for the system. Typically, a hospital's liquidity position provides a rating cushion for one-off events with limited operational and financial disruption.

Often, longer-term recovery expenses outstrip the immediate costs associated with a cyber breach. Such expenses, including remediation and enhanced security measures, along with increased cybersecurity insurance premiums, legal costs, and staffing and compliance expenses could add to a hospital's operating costs, erode liquidity and decrease funds available for debt service. With NFP hospitals already facing greater demands on their budgets from inflation and labor costs, unexpected borrowing to bolster cybersecurity infrastructure, including updating compromised

hardware and software systems, may weaken leverage metrics and erode credit quality.