Bond Case Briefs

Municipal Finance Law Since 1971

Fitch: Relentless Cyber Attacks to Pressure NFP Hospitals' Operations

Fitch Ratings-Austin/New York-22 July 2021: Ever-increasing cyberattacks on the US public healthcare sector will place material revenue and expense pressures on not-for-profit (NFP) hospitals and health systems, Fitch Ratings says. The healthcare sector has seen a historic increase in the number and severity of cyber assaults over the past 18 months. The sector is viewed as a target-rich environment due to the large amount of sensitive data that healthcare entities maintain for patient care and operations.

Cyber-crime accelerated during the pandemic as cyber criminals took advantage of the crisis, causing immense disruption to the healthcare sector at a time when it was facing enormous patient care demands. Ransomware pay-outs and efforts to protect or "harden" healthcare systems and cyber defenses are affecting hospital financial flexibility by increasing on-going operating expenses. Attacks may also hinder revenue generation and the ability to recover costs in a timely manner, particularly if they affect a hospital's ability to bill patients when financial records are compromised or systems become locked. The recovery time and costs associated with breaches of critical data not only pose significant financial burdens but also hamper the ability of healthcare institutions to provide care, which could ultimately have human costs.

The US Department of Health and Human Services estimates that sizable cyber breaches in 2020 exposed patient data of more than 22 million Americans. Cyberattacks against US healthcare entities rose by over 55% in 2020 compared with the previous year according to the cloud security firm Bitglass. Attacks also increased in sophistication and scale, with more than a 16% increase in the average cost to recover each patient record in 2020 versus 2019. Restoration of systems to pre-attack status took an average 236 days.

Hospital and health system databases are a treasure trove of critical and sensitive patient data, which are highly sought after by cyber criminals for ransomware and double extortion schemes. In the US, patient data is considered confidential, and the maintenance and disclosure of such data are governed by patient confidentiality laws, e.g., Health Insurance Portability and Accountability Act (HIPAA), on the federal and state levels. Cyber breaches that disclose patient information carry the risk of loss of consumer confidence, litigation costs and federal enforcement actions due to regulations around patient confidentiality.

Remote work for nonessential staff opened up opportunities for infiltration, as did the sector's increased use of integrated technology, such as smart medical monitoring devices, telehealth and other virtual care capabilities. Software for such devices and heavy medical equipment such as CT scanners and MRI machines are often proprietary and designed with patient care and not necessarily cyber risk in mind. Thus, such software may not always be fully integrated in the institutional cyber defense framework. Additionally, the large costs of such equipment generally mean that institutions, particularly smaller hospitals, may rely on these devices for many years, even with outdated or unsupported software, leading to gaps in institutional security systems.

Fitch includes cybersecurity in its analysis of the sector and as part of its corporate-wide Environmental, Social and Governance (ESG) framework. Cyber risk is both a social risk in terms of safety and security, and a governance risk in terms of management effectiveness. A hospital's ESG Relevance Score would be elevated if cyber risk were deemed to be material to the rating.