New York Department of Health Issues “Urgent” Cybersecurity Warning to New York Health Care Providers Following U.S. Military Action in Iran

Client Alert | 2 min read | 07.09.25

In response to the recent U.S. strikes on Iranian nuclear facilities, the New York State Department of Health (“NYS DOH”) issued a **cybersecurity advisory** (the “Advisory”) that cautions healthcare providers, such as hospitals, treatment centers, and healthcare practitioners, of a high likelihood of increased cyberattacks and heightened cybersecurity threat activity. The Advisory follows similar **announcements** and warnings from U.S. Department of Homeland Security (“DHS”), NYS Intelligence Center (NYSIC) and the Health-ISAC (Information Sharing and Analysis Center).

The Advisory encourages health providers and organizations to tighten physical and information technology (IT) security controls to protect against known attack techniques, such as:

- **Distributed Denial of Service (DDOS)**, a harmful attempt to block access to servers or networks by flooding it with traffic;
- **Ransomware,** a type of malware software that blocks access to your computer or files and demands money to unlock them; or
- **Website Defacement**, also known as digital vandalism, when a threat actor breaks into a website and changes how it looks or what it says.

The Advisory also suggests removing operational technology (OT) connections to the public internet, changing default passwords, using strong, unique passwords, securing remote access to networks, and segmenting networks. Providers are also reminded that NYS Cybersecurity regulations require hospitals to report cybersecurity incidents to the NYS DOH no later than 72 hours after determining a cybersecurity incident has occurred.

According to DHS’s Cybersecurity & Infrastructure Security Agency (CISA), cyber attacks on the healthcare industry can be particularly harmful and significant, primarily because health care providers hold vast amounts of sensitive, regulated, and monetizable data, such as protected health information (PHI), personally identifiable information (PII), financial information, insurance information, and information related to medical research and clinical trials. PHI is permanent and personal, making it particularly valuable for identity theft, blackmail, and fraud.

At the same time, hospitals and healthcare facilities operate in environments where a system outage can compromise life-saving patient care. Their dependance on electronic health records (EHR), cloud vendors, and telehealth platforms, expands the attack surface threat actors may use to infiltrate such systems. This makes

healthcare organizations more likely to pay ransoms to restore access quickly, making them especially attractive to threat actor groups. Given these risks, cybersecurity is a patient safety issue. As such, proactive preparation is essential. Failure to prepare for or quickly respond to attacks can lead to regulatory enforcement actions, class action lawsuits, reputational harm, and loss of patient trust and revenue.

Outside counsel experienced in cybersecurity, privacy, healthcare, and government investigations can help mitigate risk while maintaining privilege.

Crowell & Moring has significant experience working with companies to address these risks, both proactively and through reactive investigations should a potential cyber event occur. For further information, please contact the team below.

Contacts

Alexis Ward
Associate
She/Her/Hers

Los Angeles D | +1.213.271.2797
award@crowell.com

Neda M. Shaheen
Associate
She/Her/Hers

Washington, D.C. D | +1.202.624.2642
nshaheen@crowell.com

Jason Johnson
Partner & CHS Managing Director
New York D | +1.212.530.1860
jjohnson@crowell.com

