# Hacking and Healing: Nation-States, Cyber Attacks, and Healthcare Law

**Legal Update**

**Hacking and Healing:**

**Nation-States, Cyber Attacks, and Healthcare Law**

Modern warfare is no longer restricted to physical battlefields and professional military. Countries like North Korea and Russia few qualms about using cyberspace to reach well beyond their physical borders to target private enterprise and the civil infrastructure of adversaries. This form of non-kinetic warfare can have a variety of aims. It can involve the "hoovering" of valu data, theft of cutting-edge technologies, or the dissemination of propaganda or misinformation to influence public opinion and governmental decisions.

In recent years, one of the most alarming aspects of cyber warfare is the targeted hacking of healthcare platforms, electronic medical records, and genomic databases. Healthcare systems are repositories of vast amounts of sensitive personal data, encompassing everything from medical records to insurance information. This makes them prime targets for nation-state acto who aim to gather intelligence, disrupt infrastructure, or steal trade secrets and new technologies.

Often, businesses are reluctant to disclose the identity of the perpetrators following a breach. For instance, in March 2024, Ch Healthcare, a subsidiary of UnitedHealth Group, became the target of a massive cyberattack. The attack disrupted healthcare payments and "the delivery of prescription drugs for hospitals and pharmacies nationwide for nearly two weeks." To prevent th hackers from disclosing sensitive patient data, it is rumored that UnitedHealth agreed to pay $22 million in cryptocurrency as ransom. Outside experts blamed ALPHV, an ill-famed ransomware group also known as Blackcat. However, UnitedHealth suspected a "nation-state associated" attack. Which one? The company did not say. But there are four countries who have a reputation for targeting healthcare: China, North Korea, Russia and Iran.

**China**

In a revealing 2014 interview on "60 Minutes," former FBI Director James Comey said that American Big Businesses fall into t categories: 'those who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese.' The following year was the infamous Anthem hack. At the time, it was the largest known data breach in U.S. history. It affected ne 80 million individuals, compromising names, birthdates, Social Security numbers, and healthcare IDs. Based on the type of techniques used to perpetrate the breach, the Department of Justice eventually fingered members of a China-Linked Group a responsible parties.

**North Korea**

During the COVID-19 pandemic, North Korean state-sponsored actors capitalized on our increased reliance on digital system launching ransomware attacks against healthcare organizations. The most notorious of these campaigns involved the use of ' ransomware. This specific malware allowed the attackers to selectively encrypt files after exfiltrating valuable data for the purp of extortion. (In a cybersecurity context, "exfiltrate" refers to the unauthorized transfer of data from a computer or server to an location.) In May 2022, the FBI managed to recover Bitcoin ransom payments paid by Kansas and Colorado health care provi However, *nota bene*: In a joint statement, the "FBI, CISA, and Treasury highly *discourage* paying ransoms as doing so does n guarantee files and records will be recovered and may pose *sanctions* risks."

**Russia**

One of the most disruptive cyberattacks attributed to Russian actors is the NotPetya malware incident in 2017. Initially targetin Ukraine, the malware inadvertently spread globally, affecting various sectors including U.S. healthcare providers, leading to

massive disruptions and data losses. However, amid the ongoing Russo-Ukrainian War, healthcare providers are increasingly worried about being deliberately targeted. The American Hospital Association (AHA) voiced concerns about retaliatory cyberattacks from Russia targeting U.S. healthcare systems in response to U.S. military support for Ukraine. Although interna humanitarian law, codified in instruments such as the Geneva Conventions of 1949 and their Additional Protocols, prohibits at on purely civilian targets during armed conflict, the novelty and anonymity of cyber warfare present significant challenges in h perpetrators accountable.

**Iran**

Since the October 7th, 2023, attack by Hamas—an organization sponsored by Iran—Iran's cyber activities have escalated significantly. These attacks initially focused on Israeli healthcare facilities, such as the Barzilai Medical Center and Hillel Yaffe Medical Center, observed in mid-October. However, a significant global concern has arisen as Iran has shifted its focus to tar Israeli-developed technology, regardless of location. For instance, in September 2023, "Cyber Av3ngers," an Iran-linked hack group, began focusing on products from Unitronics PLC, an Israeli developer of Industrial Control Systems. These systems ar essential for managing industrial environments, critical infrastructures, and medical facilities, including devices like mechanica respirators and ventilators. By December, this group had breached Unitronics systems used by the Municipal Water Authority Aliquippa, PA, and other water utilities across various states, demonstrating Iran's broad targeting strategy.

**Open-Ended Legal Issues in Cybersecurity**

Despite state actors orchestrating cyberattacks against healthcare entities, providers still face considerable legal and financia without any immunity. Such attacks not only jeopardize patient safety but also expose healthcare organizations to long-term le challenges. This vulnerability was evident in instances like the UnitedHealth and Maui ransomware attacks, where providers l access to medical records and could not process prescriptions. Furthermore, the unknown and ambiguous long-term repercus of these data breaches add to their severity. For instance, last October, a hacker known as Golum breached the genomic data of 23andMe, a direct-to-consumer genetic testing service. The stolen data, including sensitive information about individuals of Ashkenazi Jewish and Chinese descent, was subsequently advertised on dark web forums. This breach led to speculation tha China might use the data to monitor ethnic Chinese abroad and raised concerns about an anti-semitic motive for targeting Ashkenazi Jewry. Although 23andMe was quickly hit by a class-action lawsuit over the incident, with so much uncertainty abo perpetrators' ultimate intentions, it could be years before the total impact of the cyber attack is known.

There is no ignoring the fact that healthcare platforms and genomic information databases hold immense appeal to both state non-state hackers due to their vast reservoirs of sensitive personal data. For many companies, the aftermath of cyberattacks healthcare providers highlights a complex array of legal challenges. Under HIPAA's Breach Notification Rule, healthcare prov are mandated to notify patients when their data is compromised. Numerous states have enacted specific healthcare privacy la and genetic information privacy statutes. Failure to comply with federal and state regulations can result in significant penalties the repercussions of data breaches extend beyond penalties and civil judgments; they damage trust, tarnish reputations, and inflate operational costs. Such incidents underscore the critical importance of robust cybersecurity measures, regular compliа audits, comprehensive employee training, and proactive incident response strategies to protect patient data and comply with l standards.

**Authors**:

Harry Nelson, Managing Partner, Nelson Hardiman

Yehuda Hausman, Law Clerk, Nelson Hardiman

**Nelson Hardiman LLP**

Healthcare Law for Tomorrow

Nelson Hardiman regularly advises clients on new healthcare law and compliance. We offer legal services to businesses at ev point in the commercial stream of medicine, healthcare, and the life sciences.