Indiana Executive Council on Cybersecurity

Healthcare Cyber Risk Outlook | Q2 2026

RISK LEVEL: MODERATE	PRIMARY PATHWAY: THIRD-PARTY / VENDOR	WATCH: DISRUPTION + DATA LEAK

Outlook

The healthcare and public health sector remains a high-consequence target because cyber incidents can disrupt care delivery, expose protected health information (PHI), and impact patient safety. Federal agencies, including HHS, assess that risk persists due to legacy systems, resource constraints, and reliance on interconnected technologies.

In Q2 2026, risk remains moderate, with Iranian cyber activity, exposure across the healthcare supply chain, and the increasing likelihood of indirect vendor-driven attacks expanding the potential for broader operational impact and reflecting a risk posture that is rising but not acute.

Iran-Related Threat Lens

Iran-linked cyber actors have targeted U.S. critical infrastructure sectors, including healthcare, in recent campaigns. Their operations commonly involve ransomware, data theft, and disruptive activity.

U.S. government reporting indicates these actors:

- Exploit unpatched internet-facing systems and weak authentication
- Target third-party service providers to gain downstream access
- Conduct “hack-and-leak” operations to amplify impact

In March 2026, a cyber group likely linked to the Iranian government claimed responsibility for a disruptive cyberattack against U.S.-based medical technology company Stryker, reinforcing risk to healthcare organizations that rely on shared vendors and externally managed systems.

Top Q2 Scenarios

- **Vendor compromise**: Access via suppliers, MSPs, or remote support channels
- **Hack-and-leak operations**: Data theft and public release to drive pressure
- **Service disruption**: Claims processing, scheduling, imaging, lab systems, or connected medical devices
- **Follow-on extortion**: Stolen access or credentials enable ransomware deployment or resale

Immediate Actions for Leadership

- **Prioritize critical vendor review**: Identify third parties with privileged access, remote connectivity, or systemic importance
- **Strengthen third-party access controls**: Require phishing-resistant MFA, unique credentials, time-bound access, and full logging
- **Reduce external attack surface:** Patch internet-facing systems and eliminate default or shared credentials, including in Internet of Medical Things (IoMT) environments
- **Validate downtime readiness**: Test contingency plans for vendor outages, including patient safety procedures and executive communications
- **Leverage available state resources:** Utilize Indiana’s *Healthcare Cyber in a Box* toolkit to support baseline cybersecurity practices and preparedness

Please contact David Ayers at: cyberhub@iot.in.gov for inquiries or to share your healthcare cybersecurity story or incident for potential inclusion in future quarterly newsletters. Anonymity is optional.