American Hospital Association™
Advancing Health in America

Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field

The cyberattack on Change Healthcare in February 2024 disrupted health care operations on an unprecedented national scale, endangering patients' access to care, disrupting critical clinical and eligibility operations, and threatening the solvency of the nation's provider network. It demonstrated that the national consequences of cyberattacks targeting mission-critical third-party providers can be even more devastating than when hospitals or health systems are attacked directly.

Incident Overview

Attack target: Change Healthcare, a subsidiary of UnitedHealth Group, is the predominant source of more than 100 critical functions that keep the U.S. health care system operating. It annually processes 15 billion health care transactions — touching 1 in every 3 patient records — including insurance eligibility verification and authorization, drug prescriptions, claims transmittals and payment.

What happened: On Feb. 21, 2024, an attack by the Russian ransomware group ALPHV BlackCat encrypted and incapacitated significant portions of Change Healthcare's functionality.

Impact: The attack had significant care delivery and financial consequences for patients, providers and communities, endangering patients and threatening the solvency of U.S. health care providers. Every hospital in the country felt the impact, either directly or indirectly. Impacts varied depending on factors such as amount of cash reserves, vendor redundancy and reliance on Change Healthcare technology.

A March 2024 AHA survey of nearly 1,000 hospitals found:

- 74% reported direct patient care impact, including delays in authorizations for medically necessary care.
- 94% reported the attack impacted them financially.
- 33% reported the attack disrupted more than half of their revenue.
- 60% reported requiring two weeks to three months to resume normal operations once Change Healthcare's full functionality was re-established.

Many providers were forced to seek alternate ways — including pulling from reserves or taking out private loans — to pay clinician and care team salaries, acquire necessary medicine and supplies, and pay for critical physical security, dietary and environmental services contract work. The need to rely on less efficient manual processes in place of electronic ones also added substantial administrative costs.

AHA response: The AHA mobilized swiftly and served as a leading voice in the entire health care sector during the crisis. To facilitate collaboration, provide input and secure support, the AHA immediately engaged with top contacts at the White House, Congress, FBI, the Department of Health and Human Services (HHS) and Cybersecurity and Infrastructure Security Agency (CISA).

As UnitedHealth Group downplayed the severity of the event over the ensuing weeks, the AHA, among other actions, consistently set the record straight, informed the media and testified before Congress. These efforts ensured that Change Healthcare, not hospitals, bore responsibility for notifying patients of any data breach.

According to Kodiak Solutions, a revenue cycle data analytics firm, **the attack caused the value of claims submitted to drop $6.3 billion for their 1,850 hospital and 250,000 physician clients alone in just the first three weeks after the attack.**

American Hospital Association™
Advancing Health in America

Lessons Learned

In 2024, over 150 million Americans have been impacted by hacks of PHI. This represents **a nearly 600% increase since 2020**, including a **nearly 300% increase in ransomware attacks**.

Third-party cyber risk is the most significant and disruptive cyberthreat to health care. The Change Healthcare cyberattack was the most consequential and debilitating cyberattack on health care in the history of the U.S. Coupled with the sharp uptick in third-party breaches in the past two years, the cyberattack made it clear that cybercriminals are seeking to maximize disruption to care delivery — by targeting mission-critical service providers and suppliers. These disruptions often cause delays to care delivery resulting in a risk to patient safety, especially in emergency situations. On October 24, 2024, Change Healthcare officially reported to the HHS Office for Civil Rights that the protected health information of *100 million Americans was stolen from Change Healthcare during its ransomware attack, making it the largest healthcare data breach in American history.*

Ninety-five percent of the most significant health sector data breaches in 2023 and 88% in 2024, defined by those where over 1 million records were exposed, were from business associates, third parties, health plans and non-hospital health care providers. Malicious actors, primarily Russian-speaking ransomware groups, have adopted a highly effective "hub and spoke" strategy. By gaining access to the hub, a third party's technology, they also gain access to all the spokes — the thousands of health care organization customers that depend on that third-party provider.

This has become a preferred strategy for at least two reasons. One, the more widespread and crippling the impact, the higher the ransom cybercriminals can demand, and the more likely victims will pay it. Two, individual hospitals and health systems have succeeded in enhancing their cyber defenses, making them more challenging targets.

> If there was ever any question that the intent of these gangs was to harm patients, it is clear now that is their fundamental intent. These ransomware attacks are not data crimes, but life-threatening violent crimes. **The ransom demand is in fact an extortion based upon the risk to patient safety.**
>
> – **John Riggi**
> AHA National Advisor for Cybersecurity and Risk

Future health care cyberattacks are inevitable in light of these highly sophisticated, evolving and relentless cybercriminal tactics. Providers need an effective third-party risk management program that:

- Identifies and prioritizes risks posed by every third-party vendor and subcontractor.
- Incorporates third-party risk-based controls and cyber insurance requirements.
- Consistently communicates these risk management policies internally.

An immediate, coordinated response is essential. Governmental health care agencies lacked familiarity with the massive scope of Change Healthcare's services and the potential impact across every aspect of health care. Hospitals lacked clarity on the responsibility of the federal government to assist, and agencies such as the Centers for Medicare & Medicaid Services had limited authority to help providers quickly.

Given the intent of cyber adversaries to disrupt health care delivery systemically, cyber preparedness is a multi-stakeholder responsibility. The AHA continues to build trusted relationships with government partners and cultivate channels for the exchange of cyberthreat information to deter cybercriminals as well as ensure a strong, swift response in case of attack.

In addition, the AHA strongly urges government partners to use all their capabilities — including military and intelligence offensive cyber capabilities — to prevent attacks as well as assist when attacks occur. Recognizing that defense is critical but insufficient, the federal government and allied nations must increase the risk and consequences for cyber adversaries.

Response and recovery plans should ensure clinical and business continuity for at least 30 days. The Change Healthcare attack underscores that cyberattacks are increasing in frequency and severity, highlighting the emerging and urgent need for hospitals to be able to sustain care delivery and operations, without core technology systems, **for four weeks or longer.**

Achieving this goal involves enhancing clinical, operational and financial downtime and backup processes as well as training all staff in the manual procedures essential to continuing operations and care delivery.

> In some ways, cybercrime is like a chronic disease. It may not be curable, but **it can be managed, and the risk of becoming "infected" can be reduced** if all parts of the health care sector and the government share responsibility...
>
> – **Rick Pollack**
> AHA President and CEO

These steps should be part of a multi-faceted, integrated approach to cybersecurity that includes mapping the cascading impact of the loss of technology and third-party provider services. The strategy also should align with the Department of Health & Human Services (HSS) voluntary **Cybersecurity Performance Goals** that the AHA helped develop and recommends all hospitals adopt.

In addition to addressing action on the organizational level, response and recovery plans must extend to regional preparedness to assist with patient care and operational function as needed in a far-reaching attack.

The Critical Need to Mitigate Risk

The far-reaching, long-lasting impact of the Change Healthcare attack highlights the ongoing challenges cybercrime poses for the health care sector. It reinforces the urgency of bolstering cyber defenses at the provider, regional and systemic levels while concurrently optimizing the ability to respond quickly in case of attack.

Key Findings and Strategic Risk Considerations for Health Care Leaders

- The merger of UnitedHealth Group, Change Healthcare and Optum created a concentration of systemic, mission-critical business and clinical services that became an operational "utility" for the entire health care sector. This led to a concentration of risk for the entire health care system as organizations became overdependent on the group's services.
- Most health care organizations' advanced enterprise risk management (ERM) programs failed to identify dependency on UHG/Change as a risk — as a mission-critical, single point of failure.
- Having seen their overdependence on Change Healthcare and its technology, it is clear that health care organizations need diversification and redundancy in their mission-critical service providers.
- Restrictive exclusivity clauses by Change Healthcare increased risk to the sector and individual customers.
- When Change Healthcare went dark, there was a lack of understanding of the cascading effects and impact on business and clinical operations.
- This lack of understanding highlights the need to map impacts and prepare sufficient downtime procedures for a loss of mission-critical services, technology and supply chain operations for 30 days or longer.

Strategic Review and Considerations of Third-Party Risk Management and ERM Programs

Hospitals and health systems should develop a dynamic, ongoing third-party risk management (TPRM) program including a multi-disciplinary governance committee made up of operational, clinical, legal, IT, cyber and privacy committee members and designating an accountable executive. TPRM is critically important for hospitals and health systems of all sizes. As such, hospitals and health systems that lack the necessary in-house expertise or resources should seek outside partners' assistance to help build and maintain their TPRM program.

The committee should evaluate new vendors and business associates based upon technical and strategic risk according to a number of factors including but not limited to:

- Life, mission and business criticality.
- Storage or access to sensitive data.
- Network access – privileged access.
- Foreign operations and subcontractor risk.
- Technical cybersecurity posture.
- Aggregate risk from the third party.

The TPRM committee should then risk-prioritize vendors and business associates and develop scalable and evolving:

- Risk-based cybersecurity requirements.
- Risk-based cyber insurance requirements.
- Breach notification requirements.

All risk-related requirements should be included in business associate agreements. Third-party and business associate contracts should also avoid exclusivity clauses for life-critical and mission-critical services, technology and supplies in the interest of patient and community safety.

Additional Recommendations

Integrate plans. Coordinate cyber incident response, emergency management, incident command, business-continuity and disaster recovery plans. Ensure that business continuity plans address both clinical continuity and operational continuity during a partial or full loss of mission-critical technology.

Address readiness, response, resiliency and recovery (4Rs). The cyber incident response plan should be developed on an organization-wide basis and define system-level, hospital-level and department-level actions. The plan should encompass all IT, operational, business and clinical functions to be addressed during the incident and post-incident recovery.

Develop regional readiness, response, resiliency and recovery plans (5Rs). A comprehensive regional incident response and communication plan should be developed for a high-impact cyberattack having regional impact on health care delivery. It should leverage preparedness plans and mutual aid agreement and include contingencies for accommodating diversion of patients and functions between facilities and assisting impacted facilities by providing personnel, communications, medical devices and technology.

Ensure downtime procedures are in place to sustain operations without core technology systems for at least four weeks. Define clinical, operational, financial and administrative downtime processes and train to ensure proficiency of staff on all shifts.

Designate downtime coaches and safety officers to support staff who may not be proficient in manual downtime procedures. Losing EMR/EHR access, including embedded safety and treatment protocols, may disrupt and delay health care delivery and increase risk to patient safety.

Identify clinical and mission-critical third-party services and establish downtime procedures if their services are unavailable. Procedures, which can include manual work and backup strategy, should be set up to sustain clinical and business operations for at least four weeks.

Evaluate network backup status, segmentation and security. There should be a regular cadence of vulnerability and penetration testing of backups. Review, document and communicate estimates of network restoration time objective and restoration point objective.

Document, designate and delegate authorities (3Ds) to make independent, high-impact decisions during a cyber incident under defined "triggers" or urgent circumstances such as organizational disconnection from the internet. Specify leadership escalation, incident command activation and staff notification protocols.

Define and document both internal impact and external dependencies impact. Map clinical, operational, and administrative impact of decisions related to shut down of internal network or internet disconnection. Document this impact and incorporate it into a response plan for leadership. For external dependencies, pay particular attention to clinical dependencies, which may be disrupted by a ransomware attack against your organization and unavailability of your network.

Review business associate agreement and cyber insurance coverage. Determine whether coverage is sufficient based on risk profile and current cybersecurity posture. In addition, examine cyber insurance requirements in business associate agreements (BAA) to ensure that they scale with the level of cyber risk presented by the business associate. It is also important to ensure all incident reporting requirements are clearly defined in all BAAs and cyber insurance contracts and that those requirements align appropriately with internal hospital and health system polices for cyber incident reporting. It is recommended that cyber incident reporting requirements be more stringent for life critical and mission critical business associates and third-party providers, for patient and community safety reasons. For example, it is recommended that these providers be required to report ransomware attacks which result in the disruption to their systems and/or services immediately to their health care clients.

FBI and CISA — An Important Relationship

The FBI and CISA are important partners to hospitals and health systems in the fight against cyber risk. It is important to build relationships with these agencies before an incident occurs. CISA is organized into **10 regions** across the country. Know whom to contact and how to reach them 24/7. Incorporate this information into the organizational incident response plan and be prepared to report any incident or threat quickly.

Work with your organization's general counsel and outside counsel on the benefits of cooperation with these entities; have them understand the civil, regulatory and Freedom of Information Act protections offered under the Cybersecurity Sharing Act of 2015 before an incident occurs. At the same time, understand what these entities can and cannot do for you.

When reporting an incident, contact with any of these three entities will automatically inform the other two.

HHS
Assistant Secretary for Preparedness and Response

Email: **CIP@hhs.gov**

FBI
Report to local field office or to
Email: **CIP@hhs.gov**
Phone: (855) 292-3937
Online: **IC3.gov**

CISA
Report to local field office or to
Email: **Central@cisa.dhs.gov**
Phone: (888) 282-0870
Online: us-cert-cisa.gov/report

Valuable Resources

CISA provides a **secure portal** for the reporting of incidents, phishing attempts, malware and vulnerabilities.

Take advantage of the **free services** offered by CISA and threat information exchange with the FBI.

Regularly review **threat notifications**.

Invite a CISA representative to speak to your executive team.

The AHA is committed to actively protecting patients, providers and the health care infrastructure through a coordinated, comprehensive approach. For more information about cybersecurity resources, free and discounted services from AHA's trusted cybersecurity providers, and access to the latest alerts and reports, visit the **AHA Cybersecurity Webpage**.