

Communications Strategy and Plan for the 2024 Change Healthcare Cyber Incident

Submitted by: Ankit Pradhan

Course: Cybersecurity Incident Communications

Section: A

Date: December 4, 2025

Professor: Ionut Anghelache

Company: Change Healthcare (UnitedHealth Group)

Table of Contents

INTRODUCTION.....	3
SUMMARY OF THE INCIDENT	4
BEST COMMUNICATION PRACTICES AND PLAN.....	5
PHASE ONE – BEFORE AN ATTACK.....	5
PHASE TWO – DURING THE ATTACK	12
PHASE THREE – AFTER THE ATTACK	16
IMPACT(S) ON THE ORGANIZATION	22
CONCLUSION.....	24
REFERENCES.....	26

INTRODUCTION

Change Healthcare, a major subsidiary of UnitedHealth Group, is one of the largest healthcare technology and payment processing companies in the United States. Headquartered in Nashville, Tennessee, Change Healthcare operates a critical infrastructure platform that processes approximately half of all U.S. medical claims, manages eligibility verification, pharmacy switching services, and prior authorization systems connecting thousands of healthcare providers, pharmacies, health plans, and patients. [1] With such extensive reach and access to protected health information (PHI) and personally identifiable information (PII) from tens of millions of Americans, Change Healthcare represents a high-value target for sophisticated cybercriminals and ransomware operators. [2]

This report analyzes the February 2024 ransomware and data breach incident at Change Healthcare, one of the largest and most disruptive healthcare infrastructure attacks in recent history. The incident, attributed to the BlackCat/ALPHV ransomware group and related affiliates, resulted in prolonged system outages affecting claims processing, eligibility checks, and pharmacy services nationwide, while exposing the personal data of over 110 million individuals to potential identity theft and fraud. [3], [4] The breach demonstrates critical cybersecurity and communications challenges faced by critical infrastructure providers and the need for integrated incident response and stakeholder communication strategies before, during, and after such attacks.

SUMMARY OF THE INCIDENT

The Change Healthcare cyber incident began with an unauthorized intrusion into the company's internal systems between approximately **February 17 and 20, 2024**, which was discovered by the company on **February 21, 2024**. [3] Attackers associated with the BlackCat ransomware group and affiliated criminal entities gained access to Change Healthcare's network, moved laterally across multiple systems, and systematically exfiltrated a substantial volume of sensitive data over several days before encrypting critical systems and rendering key services inaccessible. [2], [4]

Upon discovery, Change Healthcare immediately began containment activities by disconnecting affected systems to prevent further spread of the ransomware, leading to significant operational disruptions across the healthcare ecosystem. [5] The company's initial investigation confirmed that a significant amount of data had been stolen from its network by **March 7, 2024**, though detailed analysis was delayed until **March 13, 2024** when investigators obtained a forensic copy of the exfiltrated dataset for thorough review and impact assessment. [3]

The stolen dataset contained extremely sensitive personal information including names, dates of birth, Social Security numbers, insurance identification numbers, clinical and claims information, billing details, and guarantor information from affected individuals. [3], [6] Initial data analysis revealed that up to one in three Americans—potentially **over 110 million people**—could have been impacted by the breach, making it one of the largest healthcare data breaches on record. [3], [4] The data was obtained by BlackCat affiliates who retained copies, and competing criminal

groups including RansomHub claimed to possess or have acquired the dataset, multiplying the risk of repeated extortion attempts and data re-sale. [3], [5]

Change Healthcare posted a substitute data breach notice on its website in compliance with regulatory notification requirements and announced that affected individuals would begin receiving notification letters and emails starting **July 20, 2024**, while acknowledging that additional affected individuals might still be identified as the data review progressed. [3] In response to the breach, the company offered two years of complimentary credit monitoring and identity theft protection services to all affected individuals, established a dedicated support website at changecybersupport.com, and provided a toll-free hotline at (888) 846-4705 for victims to register for protective services and seek assistance. [3]

BEST COMMUNICATION PRACTICES AND PLAN

PHASE ONE – BEFORE AN ATTACK

1) Incident and Communications Team

Before a cyber incident occurs, a critical infrastructure organization like Change Healthcare must establish and regularly activate a formal, cross-functional cyber incident response and crisis communications team that includes senior executives, security professionals, legal counsel, and communications specialists. [2], [5] This team should comprise:

- **Executive Leadership:** Chief Information Officer (CIO), Chief Operating Officer (COO), Chief Executive Officer (CEO), and Board Representatives to provide strategic direction and authorization. [2]
- **Security and Technical:** Chief Information Security Officer (CISO), Security Operations Center (SOC) Director, Incident Response Lead, and Infrastructure/Applications Team Leads to manage technical containment and forensics. [5]
- **Legal and Compliance:** General Counsel, Privacy Officer, Compliance Officer, and Regulatory Affairs to manage legal obligations, regulatory notifications, and litigation strategy. [2], [4]
- **Communications:** Chief Communications Officer, Media Relations, Internal Communications, and Investor Relations to coordinate public messaging, stakeholder updates, and reputation management. [5]
- **Support Functions:** Human Resources, Customer Support Leadership, Third-Party/Vendor Management, and Healthcare Provider Relations to address internal needs and stakeholder concerns. [2], [5]

Clear role definitions must specify decision-making authority, communication workflows, who serves as external spokesperson to media and regulators, who coordinates with law enforcement and FBI, who drafts and approves public statements, and who manages notifications to patients, providers, and partners. [2], [4]

2) Prioritized Information Assets

Change Healthcare and similar critical infrastructure organizations must maintain and regularly update a prioritized inventory of information assets with clearly assigned business impact ratings and owner accountability. [5], [6] For a healthcare claims processor, top-priority information assets include:

- **Core Transaction Platforms (Tier 1 Critical):** Claims clearinghouse and adjudication engines, pharmacy switching networks, eligibility and benefits verification systems, prior authorization platforms—any disruption to these services directly impacts patient care and provider revenue. [2], [4]
- **Data Repositories (Tier 1 Critical):** Databases containing protected health information (PHI) including medical records, claims history, diagnoses, and treatments; personally identifiable information (PII) including Social Security numbers, dates of birth, addresses, and phone numbers; insurance and enrollment data; and beneficiary financial details. [3], [6]
- **Identity and Access Management (Tier 1 Critical):** Single sign-on (SSO) systems, multi-factor authentication (MFA) platforms, privileged access management (PAM) tools, and directory services that control who can access critical systems and data. [5]
- **Financial and Payment Systems (Tier 1 Critical):** Provider payment platforms, patient billing systems, accounts payable, cash management systems, and risk-sharing arrangement tools. [3], [4]

- **Third-Party Integrations (Tier 2 High):** APIs and data exchanges with hospitals, health plans, pharmacies, government programs (Medicare/Medicaid), other clearinghouses, and business partners. [2], [5]

Each asset should be mapped to a primary and secondary owner who can quickly provide status updates, scope of compromise details, and restoration timelines during an active incident. [4], [5]

3) Stakeholder Identification

A comprehensive pre-attack communications plan must clearly identify all key stakeholder groups, understand their information needs, and establish preferred communication channels for each group. [2], [6] For a critical healthcare infrastructure provider, stakeholders include:

- **Patients and Members:** Individuals whose claims are processed and whose personal and health data may be exposed, requiring clear information about potential identity theft risk and protective measures. [3], [6]
- **Healthcare Providers:** Hospitals, clinics, urgent care centers, and physician practices that depend on Change Healthcare for claims submission, eligibility verification, and payment processing—disruptions directly impact cash flow and patient care workflows. [2], [4]
- **Pharmacy Networks:** Community pharmacies and pharmacy benefit managers that use Change Healthcare platforms for prescription processing and reimbursement. [5]
- **Health Plans and Insurers:** Insurance companies and employer groups that depend on accurate claims data and timely payment processing; concerned about service restoration and financial impact. [2], [4]

- **Government Programs:** Centers for Medicare & Medicaid Services (CMS), state Medicaid agencies, Veterans Administration, and other government healthcare programs relying on claims processing and data integrity. [4], [5]
- **Employees and Contractors:** Internal staff and third-party vendors who need clear guidance on operational changes, security protocols, and personal data protection measures. [2], [5]
- **Regulators and Investigators:** HHS Office for Civil Rights (OCR), state attorneys general, law enforcement agencies (FBI), and other regulatory bodies overseeing healthcare privacy and cybersecurity. [4], [6]
- **Investors and Financial Community:** Stock analysts, rating agencies, institutional investors, and financial advisors concerned about operational impact, financial losses, and long-term business viability. [3], [4]
- **Media and General Public:** News organizations, healthcare industry media, and the general public, whose perception influences organizational reputation, customer/partner confidence, and regulatory scrutiny. [2], [6]

4) Technologies, Safeguards, and Controls

Robust security controls serve a dual purpose: they reduce the technical risk of successful attacks while also providing the technical foundation for credible communications during and after an incident. [5], [6] Essential safeguards include:

- **Strong Identity and Access Management:** Mandatory multi-factor authentication (MFA) for all remote access, critical system access, and privileged accounts; least-privilege access principles limiting each user to minimum necessary permissions;

continuous credential hygiene including regular rotation and anomaly detection; and conditional access policies blocking suspicious login attempts. [2], [5]

- **Network Segmentation and Zero-Trust Architecture:** Micro-segmentation dividing the network into security zones so that compromise of one environment (e.g., email systems) does not cascade to critical systems (e.g., claims processing); zero-trust architecture requiring verification of every access request regardless of source; and strict controls on data flows between network segments. [2], [5]
- **Data Protection:** Encryption of protected health information (PHI) and personally identifiable information (PII) both at rest (in databases and storage) and in transit (during transmission between systems); strong key management including hardware security modules and key rotation; and masking of sensitive data in non-production environments. [3], [4], [6]
- **Comprehensive Monitoring and Visibility:** Security information and event management (SIEM) platforms aggregating logs from all systems; endpoint detection and response (EDR) tools identifying suspicious process behavior and malware; network traffic analysis detecting data exfiltration; and threat hunting capabilities proactively searching for attacker indicators. [5], [6]
- **Tested Backup and Disaster Recovery:** Regular, tested backup procedures with multiple copies stored in geographically distributed, physically isolated locations; immutable (write-once, read-many) backups that attackers cannot encrypt or delete; and documented recovery procedures that are regularly exercised to ensure actual restoration capability, not just assumed capability. [2], [4]

- **Vulnerability Management:** Regular vulnerability scanning of all systems; timely patching of identified vulnerabilities prioritized by criticality; and formal change management processes preventing unauthorized system modifications. [5]
- **Security Incident Response Drills:** Quarterly or semi-annual tabletop exercises simulating ransomware attacks, data theft, and extortion scenarios, with participation from executives, technical leads, legal, communications, and key stakeholders; and after-action reviews documenting findings and improvements. [5], [6]

5) Internal and Third-Party Reporting Process

Effective incident detection depends on creating simple, accessible channels for employees, contractors, vendors, and partners to report suspected security incidents without fear of retaliation. [2], [5] This process should include:

- **Multiple Reporting Channels:** Dedicated security incident email address (e.g., security-incident@changehealthcare.com); 24/7 security hotline with direct connection to Security Operations Center; clear guidance in employee handbooks and security awareness training; and pre-defined "Security Incident" ticket categories in IT helpdesk ticketing systems. [5], [6]
- **Clear Reporting Guidance:** Simple, one-page guidance describing what to report including suspicious emails (especially those requesting credentials or containing unusual links), unexpected multi-factor authentication prompts, unusual system behavior, attempts to access data outside normal job function, and suspected data leaks; real-world examples and phishing simulations demonstrating what to watch for. [2], [5]

- **Non-Retaliation Policy:** Formal, communicated policy explicitly protecting reporters of suspected incidents from any adverse employment action; reinforcement by executive leadership during security awareness campaigns; and transparent processes for handling reports ensuring no conflict of interest in evaluation. [5]
 - **Formal Escalation Process:** First-line support or local IT → Security Operations Center → Incident Response Lead → Executive Steering Committee for potential breach classification and external notifications, with defined timelines (e.g., escalation within 1 hour to SOC, within 2 hours to IR Lead, within 4 hours to Executives). [2], [4], [5]
-

PHASE TWO – DURING THE ATTACK

1) Cause of the Incident

During an active cyber incident, the technical cause must be rapidly but carefully assessed and documented to support forensic analysis, regulatory notifications, and communications to stakeholders. [4], [5] In the Change Healthcare case, attackers associated with the BlackCat/ALPHV ransomware group and related affiliates infiltrated internal systems, likely through compromised credentials or exploitation of an external-facing application vulnerability. [2], [4] The attackers maintained access over several days (February 17-20, 2024), moved laterally across network segments to expand their access, and systematically exfiltrated multiple terabytes of sensitive data before deploying ransomware that encrypted critical systems and forced disconnection of key services. [3], [4]

In public communications, the organization should explain the general nature of the attack (e.g., "ransomware with associated data exfiltration"), clarify what is known and unknown at that point in time, and explicitly avoid speculation about attack methodology or attribution until forensic analysis is mature and verified. [4], [5] Premature or inaccurate attribution claims can undermine credibility when later corrected. [5]

2) Evidence Captured

Throughout an active incident, technical teams must systematically capture and preserve forensic evidence to support investigation, law enforcement cooperation, breach notifications, and potential litigation. [5], [6] Critical evidence categories include:

- **Access Logs:** VPN and authentication server logs showing login patterns, source IP addresses, and timing; identity provider logs showing MFA success/failure and anomalous access patterns; and application logs showing which accounts accessed which data and when. [5]
- **Endpoint Telemetry:** Process execution histories from compromised systems showing attacker tools and lateral movement; file access logs showing data accessed and copied; and memory forensics capturing malware characteristics. [6]
- **Network Forensics:** Network flow data showing data exfiltration volumes and destinations; firewall logs showing unusual outbound connections; and DNS query logs showing command-and-control communication. [5]
- **Malware and Attack Artifacts:** Samples of ransomware executables and decryption tools; copies of ransom notes and extortion communications; screenshots of attacker activities; and evidence of data staging and exfiltration infrastructure. [5], [6]

- **Timeline Reconstruction:** Detailed chronology of attack discovery (February 21, 2024), initial data confirmation (March 7, 2024), and forensic analysis completion (March 13, 2024), establishing the scope and duration of attacker presence. [3], [4]

In the Change Healthcare case, investigators reconstructed that attackers had access for 3-4 days before discovery, exfiltrated terabytes of data encompassing records of over 110 million individuals, and that multiple criminal groups (BlackCat affiliates, RansomHub) obtained copies, which has informed regulatory inquiries, notifications, and ongoing law enforcement investigations. [3], [4]

3) Adequacy of Pre-Attack Plan

The organization should conduct a critical assessment of whether its pre-defined communication and incident response plan would have been adequate for this type and scale of breach. [2], [5] A mature plan would have enabled:

- **Rapid Team Activation:** Immediate convening of executive incident team and communications working group within 1-2 hours of detection, rather than delays caused by executive travel, decision-making paralysis, or unclear authorities. [4], [5]
- **Fast Initial Notifications:** Pre-approved templates for initial "holding statements" to media (within 4-6 hours of public awareness of incident) and notifications to critical stakeholders (providers, payers, regulators) within defined timeframes (often mandated by regulation). [4], [5]

- **Stakeholder-Specific Communications:** Tailored messages for each stakeholder group prepared rapidly from templates, avoiding "one-size-fits-all" messaging that fails to address specific concerns of providers, patients, regulators. [2], [5]
- **Clear Decision Criteria:** Predetermined criteria for classifying incident severity, triggering external notifications, engaging law enforcement, and escalating to board level, enabling rapid decisions under stress rather than protracted debate. [4], [5]

In practice, the Change Healthcare breach illustrates where communication timelines were challenged: while the intrusion was discovered on February 21, 2024, comprehensive notification to all affected individuals was not completed until months later (with notifications beginning July 20, 2024, and continuing through late 2024), drawing significant criticism from regulators, media, and affected individuals who felt left in the dark about data theft and identity theft risk. [3], [4] Legal actions and investigations have since questioned whether faster and clearer initial disclosure would have better served the public and mitigated reputational damage. [2], [5]

An **Incident Checklist During Active Attack** should include:

- Immediate incident severity declaration (Critical/High/Medium/Low)
- Activation of incident response team and crisis communications team
- Isolation of affected systems to prevent further spread
- Engagement of external incident response and forensic investigators (if not in-house)
- Notification to senior executives and board leadership within 2-4 hours
- Initial notification to FBI/CISA and coordination with law enforcement

- Drafting and approval of holding statement for media (within 4-6 hours if public knowledge)
- Preparation of FAQs for customers, providers, and internal staff
- Setup of dedicated incident website with latest information and support resources
- Establishment of 24/7 incident command center coordinating technical, communications, legal, and business operations teams
- Regular (daily or twice-daily) stakeholder update calls with pre-planned talking points
- Documentation of all decisions, communications, and forensic findings in a centralized incident log

PHASE THREE – AFTER THE ATTACK

1) Information to Monitor and Communication Methods

After initial containment and system restoration begins, the organization must establish systematic monitoring of multiple information streams and adjust communications accordingly.
[4], [5], [6]

Information to Monitor:

- **System Recovery Status:** Progress on patching vulnerabilities, restoring systems from clean backups, and returning services to full functionality; metrics tracking percentage of systems restored and performance metrics (claims processing volume, system uptime).

[4], [5]

- **Ongoing Threats:** Indicators of attempted re-entry by attackers, new vulnerabilities discovered in compromised systems, insider threats from disgruntled employees, and suspicious access patterns suggesting persistent attacker presence. [5], [6]
- **Data Exposure:** Monitoring of dark-web forums and criminal marketplaces for appearance of stolen data or announcements of data sales; tracking of competing criminal groups (RansomHub, etc.) claiming possession of data; and monitoring of leaked data repositories for misuse. [3], [4]
- **Regulatory and Legal Activity:** Notifications of investigations from HHS OCR, state attorneys general, and law enforcement; service of legal complaints in breach-related lawsuits; and class-action certification petitions. [2], [4], [5]
- **Media and Social Sentiment:** Media coverage tone and messaging accuracy; social media conversations about the breach among patients, providers, and industry observers; and sentiment analysis of public perception. [2], [5]
- **Stakeholder Feedback:** Provider concerns about claims processing restoration and financial support; patient questions about identity theft risk and credit monitoring; investor concerns about operational risk and financial impact; and employee morale issues related to layoffs or operational changes. [2], [4]

Communication Methods by Stakeholder:

- **To Affected Patients/Members:** Individualized notification letters via U.S. mail (required by most state laws) plus email notifications; dedicated website with FAQ, credit monitoring registration, and support resources; toll-free hotline with live support agents; and SMS alerts for time-sensitive updates. [3], [4], [6]

- **To Healthcare Providers:** Webinars and conference calls with Q&A; dedicated provider portal with real-time claims processing status; provider newsletters with regular updates; and direct outreach from provider account managers. [2], [5]
- **To Health Plans and Payers:** Executive briefing calls; detailed incident reports; impact assessments on claims data accuracy; and coordination meetings on provider support strategies. [4], [5]
- **To Employees:** Town halls with CEO and incident leadership; internal website with incident updates and FAQs; internal newsletters and email updates; and mental health and employee assistance resources given operational stress. [2], [5]
- **To Media:** Press releases on major milestones (system restoration, forensic investigation completion); media interviews by CEO and company spokesperson; press briefings addressing media questions; and background briefings for healthcare industry reporters. [2], [4]
- **To Investors:** Earnings calls with detailed impact disclosures; SEC filings (10-K and 10-Q) documenting financial impact; investor letters from CEO; and direct investor relations outreach. [3], [4]
- **To Regulators:** Regular submission of incident updates to HHS OCR; cooperation with investigations by state attorneys general and law enforcement; and participation in regulatory inquiries and congressional briefings. [4], [5], [6]

2) Litigation Communication

Large healthcare data breaches inevitably generate regulatory investigations, civil litigation (class actions and individual lawsuits), and potential enforcement actions, requiring tightly coordinated legal and communications strategies. [2], [4]

- **Consistency Between Forums:** Legal counsel and communications must ensure that messaging is consistent between public statements (press releases, website), regulatory submissions (breach notifications, audit responses), court filings (motions, settlement documents), and investor disclosures (10-Q/10-K filings, earnings calls), because contradictions undermine credibility and can be used against the company in litigation. [4], [5]
- **Coordination Protocol:** Establish clear process where all external communications are vetted by legal counsel to ensure consistency with legal strategy and to avoid inadvertent admissions of liability or facts that could harm litigation positions. [2], [4]
- **Messaging Framework:** Acknowledge the incident and its seriousness without pre-judging liability ("We are committed to supporting affected individuals and cooperating fully with regulatory investigations"); emphasize investigative progress and remedial actions taken; highlight support offered to victims (credit monitoring, dedicated hotline, financial assistance if applicable); and commit to transparency and accountability. [4], [5]
- **Settlement Communication:** If settlement is reached with regulators or in class action litigation, coordinate on messaging about settlement terms, victim compensation, and corporate commitment to enhanced security. [2], [4]

In the Change Healthcare case, the organization faces multiple lawsuits from affected individuals and state attorneys general, so maintaining disciplined, consistent messaging across all public forums is essential to managing legal and reputational risk. [2], [4], [5]

3) Cybersecurity Incident Checklist Update and Resourcing

Post-incident review (often called a "lessons learned" exercise) should systematically evaluate what worked, what failed, and what should change in future incidents. [5], [6] This review should result in updates to:

- **Detection and Escalation:** Analysis of where detection delayed and how to accelerate threat identification; assessment of whether monitoring tools detected attacker activity and why alerts were or were not acted upon; and updates to alert thresholds and escalation procedures. [5], [6]
- **Communications Timelines:** Evaluation of whether pre-planned notification timelines were realistic and appropriate; identification of bottlenecks in approval processes that delayed communications; and updates to holding statements, templates, and decision frameworks. [2], [4], [5]
- **Stakeholder Contact Lists and Channels:** Verification that stakeholder contact lists are current and accurate; testing of communication channels (email, phone, websites) to ensure they functioned under stress; and addition of new stakeholder groups or communication channels identified during the incident. [4], [5]
- **Incident Command Structure:** Assessment of whether team composition was appropriate; evaluation of decision-making processes and whether decisions were timely; and clarification of roles and authorities. [2], [5]
- **Forensic and Evidence Preservation:** Review of evidence capture processes to identify gaps; updates to procedures for securing and maintaining chain of custody; and enhancement of logging and telemetry to support future investigations. [5], [6]

Additional Tools and Resources that may be required based on incident findings:

- **Enhanced Identity Security:** Deployment of passwordless authentication, hardware security keys, and continuous authentication systems to reduce reliance on credentials as access control mechanism. [2], [5]
- **Advanced Threat Detection:** Deployment of behavioral analytics and machine learning-based anomaly detection to identify attacker activity faster than rule-based SIEM detection. [5], [6]
- **Improved Backup and Resilience:** Investment in immutable backup infrastructure, geographic distribution of backups, and rapid recovery orchestration tools enabling faster restoration of critical systems. [2], [4]
- **Expanded Incident Response Capability:** Hiring or contracting additional incident responders and forensic investigators; pre-arranged retainers with external incident response firms ensuring availability during crisis; and investment in commercial incident response platforms. [4], [5]
- **Legal and Privacy Resources:** Expanded Legal, Privacy, and Compliance teams given regulatory complexity of healthcare data breach; pre-arranged relationships with specialized healthcare privacy counsel; and expanded communications staff given scale of stakeholder notifications. [2], [4], [5]

The financial scale of impact reported by UnitedHealth Group (over USD 1 billion in incident-related costs when including response expenses, financial assistance to providers, remediation investments, and operational impact) underscores that investing substantially in incident

readiness, resilience, and comprehensive incident response is justified as a core enterprise risk management function. [3], [4]

IMPACT(S) ON THE ORGANIZATION

The February 2024 Change Healthcare cyber incident had profound ramifications extending far beyond the company itself:

- **Operational Disruption:** The attack forced disconnection of critical claims processing, eligibility, and pharmacy systems nationwide, disrupting healthcare operations for weeks and forcing providers, pharmacies, and payers to implement manual workarounds. This created immediate cash-flow crises for providers unable to submit claims electronically, delays in patient prescriptions at pharmacies, and administrative burdens on all healthcare ecosystem participants. [2], [4], [5]
- **Financial Impact:** UnitedHealth Group reported approximately USD 872 million in adverse impact to Q1 2024 operating earnings; an additional USD 800 million added to claims reserves to manage timing uncertainties; and estimated total incident costs exceeding USD 1 billion when including response expenses, provider financial support, incident response services, and remediation investments. [3], [4]
- **Reputational Damage:** The incident severely damaged Change Healthcare and UnitedHealth Group's credibility and reputation as a responsible steward of sensitive healthcare data, raising questions among providers, payers, and patients about the company's capability to safeguard critical infrastructure and personal information. [2], [3]

- **Patient Harm and Identity Theft Risk:** Over 110 million individuals' personal and health information was compromised, exposing them to heightened risk of identity theft, medical fraud, fraudulent insurance claims, phishing, and social engineering attacks. [3], [4], [6] The linking of email addresses with account profiles substantially elevated the threat level compared to publicly available information alone. [3]
- **Regulatory Scrutiny:** The incident triggered investigations by HHS Office for Civil Rights, state attorneys general, and law enforcement agencies; Congressional hearings examining the incident and systemic risks in healthcare infrastructure; and potential regulatory enforcement actions and fines. [4], [5], [6]
- **Legal Liability:** Multiple lawsuits were filed by affected individuals, state attorneys general, and business partners, exposing the company to substantial damages, settlements, and legal costs. [2], [4]
- **Industry-Wide Implications:** The incident exposed systemic concentration risk in U.S. healthcare infrastructure, where a single company's compromise can disrupt care and billing across the entire nation; prompted regulatory and congressional calls for enhanced cybersecurity requirements in healthcare; and raised awareness of ransomware and data-theft as critical healthcare risks. [2], [4], [5], [6]

CONCLUSION

The February 2024 Change Healthcare ransomware and data-theft incident represent one of the largest and most disruptive healthcare infrastructure attacks in U.S. history, affecting over 110 million individuals, disrupting claims processing and pharmacy services nationwide, imposing over USD 1 billion in costs, and raising systemic questions about the resilience and security of critical healthcare infrastructure. [3], [4], [5] The exploitation of network access by the BlackCat ransomware group, the exfiltration of massive volumes of sensitive personal and health information, the extended service disruptions, and the involvement of multiple criminal groups claiming possession of stolen data illustrate how security vulnerabilities in critical infrastructure can cascade into nationwide consequences affecting patients, providers, payers, and the entire healthcare system. [2], [3], [4]

For organizations operating critical infrastructure, this incident underscores the imperative for robust, integrated approaches to cybersecurity and communications planning. Effective incident response and crisis communications require substantial preparation before an attack—establishing clear teams and decision-making authority, prioritizing critical assets and stakeholders, deploying comprehensive technical safeguards, and practicing coordinated response through realistic exercises. [4], [5], [6] During an active incident, disciplined execution of these pre-plans, rapid escalation to senior leadership, and transparent communication to all stakeholder groups are essential to maintaining operational continuity and public trust. [2], [4], [5]

Ultimately, this breach illustrates that maintaining data security and operational resilience in today's complex, interconnected healthcare ecosystem is an ongoing challenge requiring sustained vigilance, continuous investment in security and monitoring capabilities, integrated incident response planning, transparent and timely communications with stakeholders, and accountability at all organizational levels. [3], [4], [5], [6] Organizations that successfully manage such incidents are those that have prepared extensively in advance, maintain clear communications strategies and stakeholder relationships, execute disciplined incident management, and commit to continuous improvement based on real-world experience.

REFERENCES

- [1] Beyond Identity, "Change Healthcare Data Breach: Over 110 Million Potentially Affected, Free Credit Monitoring Offered," 2024.
- [2] Holland & Knight, "Change Healthcare Cybersecurity Incident: Financial Impact and Policy Considerations," Jun. 20, 2024.
- [3] HealthCare Dive, "Change Healthcare data breach officially affects 100M," Oct. 23, 2024.
- [4] IBM, "Change Healthcare attack expected to exceed \$1 billion in costs," May 7, 2024.
- [5] CM Alliance, "Change Healthcare Ransomware Attack: A chronological timeline," Nov. 16, 2025.
- [6] Kaspersky, "The complete story of the 2024 ransomware attack on UnitedHealth," Feb. 19, 2025.
- [7] Office of Financial Research, "The Cyberattack on Change Healthcare," Nov. 12, 2024.
- [8] U.S. HHS, "Change Healthcare Cybersecurity Incident – Frequently Asked Questions," Apr. 18, 2024.
- [9] Hyperproof, "Understanding the Change Healthcare Breach," Aug. 26, 2025.

[10] American Hospital Association, "Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness," Feb. 18, 2025.