Now & Next
Healthcare Alert

November 12, 2025

The Change Healthcare cybersecurity breach: Impact on healthcare providers

By Harsh P. Parikh, Morgan C. Nighan, Valerie Breslin Montague, Mambwe Mutanuka, and April C. Yang

Here's what US healthcare operations need to know about the incident, its timeline, the pending litigation, and potential claims adjudication and relief.

What's the impact?

- Change Healthcare's systems were targeted by ransomware, affecting nearly 193 million people — the biggest healthcare data breach to date.
- The ripple effects of the outage affected claims processing, cash flow, and pharmacy transactions, necessitating costly manual solutions.
- Litigation followed, and these cases have been centralized in a multi-district litigation focused on security failures and repayment terms.

In February 2024, Change Healthcare (Change) — one of the largest healthcare administrative and payment clearinghouses in the United States, which was acquired by the UnitedHealth Group in 2022 — was targeted by a cyberattack. Change's cybersecurity failures and the resulting

cyber incident triggered a crisis with far-reaching consequences that continue to affect healthcare providers across the country. As the operator of critical infrastructure for claims submission, eligibility verification, payment processing, and pharmacy benefit transactions, Change is at the center of the data and financial underpinning of daily operations for the US health system. The scope and duration of the outages, and Change's delayed recovery of its systems, disrupted provider revenue cycles nationwide, exposed sensitive data, forced manual workarounds in care settings, and instigated a wave of litigation. These lawsuits against Change are now consolidated into multi-district proceedings in Minnesota federal court. This article summarizes what is known about Change's breach and its downstream operational, financial, and legal consequences for healthcare providers, many of which are clients of Nixon Peabody. This article also outlines the posture and stakes of the pending litigation between providers and Change.

February 2024 breach and immediate disruption

On February 21, 2024, Change detected a ransomware attack affecting systems that support electronic data interchange among thousands of providers, payors, and pharmacies across the country. In May 2024, UnitedHealth Group CEO Andrew Witty testified before the Senate that hackers gained access to Change's system on February 12, 2024, using compromised credentials on a Citrix remote access portal that lacked multi-factor authentication. The nine-day delay between the initial hack and Change's detection exposed critical deficiencies in data security and timely threat detection, which Witty acknowledged was caused in part by its failure to update internal security procedures after the acquisition of Change in October 2022. Change confirmed on March 7, 2024, that data had been exfiltrated from its systems — including health information, Social Security numbers, driver's license and passport numbers, and financial/payment card information — and Change subsequently paid (through Optum, another UnitedHealth Group subsidiary) a $22 million ransom to ensure deletion of the stolen data. Change's systems were offline beginning February 21, 2024, and did not resume functionalities for many months thereafter.

The breach impaired core transaction workflows — including claims submission, authorization, adjudication, collections, remittance, eligibility checks, and pharmacy benefit transactions — that disrupted the transmission of clinical and billing data needed to sustain care delivery and payment. Due to the scale of Change's operations in the US healthcare industry, the outage had a systemic effect: Hospitals, physician practices, laboratories, behavioral health providers, surgery centers, medical equipment suppliers, and pharmacies experienced delays, backlogs, and — in some cases — an abrupt halt to revenue inflow. Patients also reported being unable to contact Change through their patient portals or Change's patient inquiry hotline to make payments while Change's system was down.

Change's early response focused on isolating compromised systems, restoring functionality, and coordinating with federal authorities and industry partners to mitigate damage, but as systems

remained offline or degraded for an extended period, the disruption moved from an IT incident to a full-fledged operational and liquidity problem for providers that rely on predictable claims cycles to fund payroll, supplies, and other fixed costs.

Initially, Change reported to the Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) that the data breach had affected more than 500 individuals. Change later revised the estimate to 100 million, and then 190 million affected. As of July 31, 2025, Change notified OCR that its estimate had increased to 192.7 million affected individuals, representing nearly two-thirds of the US population. These metrics establish the Change data breach as the largest healthcare data breach ever recorded.

OCR's unprecedented, proactive announcement of its investigation in March 2024 — initiated before Change had even reported the breach to OCR — further underscores the scale and widespread impact of the cyberattack. OCR typically initiates investigations of cyberattacks and data breaches several months after breaches are reported, which can sometimes be years after the breaches occur. Although OCR has not announced any enforcement actions or findings as of November 2025, the timeline is not unusual for a breach of this magnitude and significant penalties remain likely.

Operational, financial, and compliance impacts on providers around the country

The downstream effects on providers of the February 2024 breach can generally be grouped into four interrelated consequences.

OPERATIONAL CONTINUITY WAS CRITICALLY COMPROMISED

With automated processes and safeguards out of commission, many providers resorted to manual claims submission and alternate clearinghouses where feasible. Pharmacy transactions faced interruptions that required ad hoc overrides or cash-pay accommodations, which strained patient access. These workarounds increased error rates; delayed revenue cycle timelines; and created reconciliation burdens that have persisted, and are likely to continue, through multiple billing cycles.

CASH-FLOW WAS INTERRUPTED

Even short delays in claims submission and payment remittance can create liquidity gaps for provider organizations with narrow margins. For many providers, claim denial rates rose due to untimely submission caused by Change's system outage and formatting errors caused by manual submissions. Smaller provider practices have been particularly burdened, encountering payroll challenges and deferral of capital and strategic initiatives, with some providers even facing risk of bankruptcy or expenditure of personal funds to keep their businesses afloat.

COMPLIANCE AND RISK MANAGEMENT COSTS INCREASED

Providers had to assess whether their own systems or business associate relationships were implicated by the data breach, evaluate their obligations to notify affected individuals,[1] and coordinate with their cyber-insurers. Heightened scrutiny of access controls, audit logging, vendor management, and incident response planning required additional investment and resource expenditure. Training and technical safeguards had to be reinforced or expanded to align with federal security standards designed to protect electronic health information, including more robust documentation of incident response and contingency planning.

LEGAL AND COMPLIANCE RISK EXPOSURE BROADENED

In addition to the burdens caused by decreased or interrupted cash flow, providers faced potential contractual disputes, patient complaints, and regulatory inquiries and investigations. Many healthcare providers find themselves in disputes with their contracted health plans and managed care networks, and continuing to face difficulties in collecting reimbursement for medically necessary services. Where data regulated under federal or state law was accessed or exfiltrated, obligations to notify patients and offer credit monitoring resulted in direct costs and potential reputational damage. In parallel, the breach prompted further resource expenditure on private litigation against Change and related entities that may affect providers' rights, recovery prospects, and continuing obligations as class members or third-parties with relevant information.

Optum's temporary financial assistance program

Ostensibly to help providers through immediate cash-flow shortages, the UnitedHealth Group, via its subsidiary Optum, established a temporary financial assistance program ("TFAP") offering an advance of funds that providers would have otherwise expected to receive were it not for the outage of Change's systems. UnitedHealth Group CEO Andrew Witty has publicly stated that providers would not be required to repay the advances until the providers determined they were financially stable and their operations were back to normal. However, participating providers have reported that Optum has begun to aggressively pursue repayment of such advances — despite the fact that these providers' business operations are still reeling from the financial damage caused by Change's outage. Many providers have not recouped amounts owed by Change and third-party payors for medical service claims that were untimely or otherwise improperly submitted as a result of Change's system failures.

[1] On May 31, 2024, HHS updated its FAQs page regarding the Change data breach to clarify that covered entities under HIPAA could delegate their breach notification obligations to Change/United.

The TFAP terms are in dispute in a class action litigation pending against Optum, Change, and affiliates.[2] The court recently admonished Optum for its misleading communications to providers and for failing to mention the ongoing litigation and the dispute over Optum's right to collect under the TFAP advances.[3]

Strategic considerations for providers

Providers navigating the aftermath of Change's breach must focus on stabilizing revenue operations by clearing backlogs of unpaid claims and normalizing transaction flows going forward. For historical claims, providers must tighten internal processes for claims denial management and adjudication. Providers are continuing to strengthen vendor risk governance, including mapping data flows, updating and enforcing incident reporting and recovery procedures, and calibrating indemnity and limitation-of-liability terms in new and existing contracts. Providers must evaluate both historical accounts receivable and how best to proceed with vendors from now on. Of note, providers must remember to preserve pending claims and documentation to support potential recoveries, insurance submissions, and responses to regulatory inquiries.

The litigation landscape of multi-district proceedings in Minnesota

The Change breach almost immediately spawned putative class actions and related suits filed in multiple jurisdictions, alleging inadequate security controls; delay or deficiency in breach notification and response; and resulting harms, including exposure of sensitive data, identity theft risks, out-of-pocket mitigation costs, and demonstrable economic losses — including lost revenues — from service disruption. The actions have been brought by patients and providers. To avoid duplicative discovery and inconsistent rulings, these cases have been centralized for pretrial coordination in a multi-district litigation ("MDL") venued in the District of Minnesota[4] — a court system frequently selected for complex data breach MDLs in the healthcare and consumer sectors.

Centralization of cases related to the Change data breach streamlines threshold motions practice, fact discovery, expert development, and class certification briefing, while leaving trial remands to the transferor courts if cases are not resolved. The key issues expected to shape the MDL proceedings include:

---

[2]See *Total Care Dental and Orthodontics, et al. v. UnitedHealth Group Incorporated, et al.*, No. 25-cv-00179 (D.M.N.).

[3]*Id.*, Dkt. 88 at p. 17–19 (granting Provider Plaintiffs' motion for court supervision of communications between Defendants and the putative class because "Defendants have engaged in misleading communications").

[4]*See In re Change Healthcare, Inc., Customer Data Sec. Breach Litigation*, No. 24-MD-03108) (D.M.N.).

- The sufficiency of Change's cybersecurity infrastructure relative to known or predictable threats;
- Terms and conditions of repayment under the TFAP;
- Causation and injury frameworks for data exposure claims;
- The measure of economic loss for downstream business interruption; and
- The interplay between federal privacy standards and state consumer protection laws.

Remedies sought include monetary damages, restitution, injunctive relief mandating security enhancements and monitoring, and attorneys' fees and costs. The outcomes at the class certification and summary judgment stages, as well as any bellwether proceedings, will influence the parties' settlement posture and the scope of prospective relief. The next status conference in the case is scheduled for November 20, 2025.

Regulatory and industry implications

Beyond the pending litigation, the Change breach is likely to continue its ripple effect in the healthcare regulatory and industry landscapes. Federal and state regulators may focus on contingency planning for third-party outages, minimum security baselines tailored to the size and complexity of entities handling health data, and improved information-sharing regarding active cyber threats. Contracting norms may shift toward more-stringent incident reporting and response timelines, more-robust audit and certification processes, clearer data segmentation and protection requirements, and expanded remedies for service disruption. By way of example, more and more providers are demanding that practice management and revenue cycle vendor management contracts include broader scope of indemnity protections (including negotiating to remove "limitation of liability" clauses), and including "without cause" termination rights so providers are not overtly reliant on a single practice management vendor.

Looking ahead

The Change data breach has emphasized the systemic interdependencies in the health data and payments ecosystem. Impacted providers will contend with operational and financial aftershocks for months, even as the MDL proceeds in Minnesota. The MDL will provide a focal point for fact investigation and legal rulings that could reshape risk allocation among data intermediaries, payors, providers, and vendors. Regardless of litigation outcomes, the cybersecurity incident has accelerated investment in the healthcare sector in cyber-resilience, vendor governance, and contingency architectures designed to maintain care delivery and cash flow in the event critical intermediaries may be compromised in the future.

Nixon Peabody currently represents a wide range of providers across the country in connection with the February 2024 cyber incident and its aftermath. We are working with both contracted and non-contracted providers requiring legal support to address consequences of the Change

cybersecurity incident, as well as communications with Change/Optum regarding transition to other billing vendors and TFAP advance repayment. Providers continuing to mitigate operational and economic damages caused by the Change breach are encouraged to consult with legal counsel regarding their ongoing relationship with Change/Optum, their potential status as putative class members of the pending class action, and preservation of their rights to claims adjudication and other relief.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Harsh P. Parikh
213.629.6108
hparikh@nixonpeabody.com

Valerie Breslin Montague
312.977.4485
vbmontague@nixonpeabody.com

April C. Yang
213.629.6003
ayang@nixonpeabody.com

Morgan C. Nighan
617.345.1031
mnighan@nixonpeabody.com

Mambwe Mutanuka
312.977.4464
mmutanuka@nixonpeabody.com