LOS ANGELES & SAN FRANCISCO

Daily Journal

www.dailyjournal.com

MONDAY, AUGUST 18, 2025

The legal fallout from the largest healthcare data breach in the U.S.

The February 2024 cyberattack on Change Healthcare, a UnitedHealth subsidiary, exposed sensitive medical data of nearly 190 million Americans, disrupted billions in claims processing, left providers financially vulnerable, sparked widespread litigation, and prompted proposed federal cybersecurity legislation -- highlighting critical gaps in healthcare IT security and multi-factor authentication practices.

By David A. Rawi

Shutterstock

In February 2024, Change Healthcare Inc., a subsidiary of UnitedHealth Group's Optum division, was hacked by a cybercriminal group calling themselves ALPHV or BlackCat in what is known as the largest healthcare data breach in the nation.

ALPHV/BlackCat breached Change Healthcare's information technology systems by gaining access through a portal that gave users remote access to desktops. From there, ALPHV/BlackCat then moved laterally through the company's systems and deployed ransomware that encrypted its patient data and prevented Change Healthcare's access to it. The group was successful because Change Healthcare's system lacked multi-factor identification – a sometimes pesky but basic security feature you encounter like when you log into your Netflix account ("Hi Bob, is that you signing in?").

This was not some small oversight with a short-lived ripple of effects. The breach has been devastating to the healthcare community in part because United and Change Healthcare are behemoths in the healthcare industry. Change Healthcare was acquired by United in approximately 2022 in a deal scrutinized by regulators and highlighted as a mega-merger with monumental impacts in healthcare. At the time of the merger, United was ranked the 5th largest company in the U.S., pulling in annual reported revenues of $324 billion. United acquired Change Healthcare because of the company's status as a healthcare information technology leader and its unique platform for claims processing, payment systems, and data analytics (think medical necessity determinations). The company processes approximately 15 billion healthcare transactions annually, which covers roughly one-third of America's patient records. So, the company's hands touch an incredible number of patient/provider medical bills containing sensitive patient information about diagnoses, medicines, test results, images, treatments, and medical histories, including for military personnel. When ALPHV/BlackCat hacked Change Healthcare, they took that information. Even after United paid ALPHV/BlackCat its multi-million-dollar ransom, United did not get the stolen data back.

In July 2024, United first reported that the breach could have affected 500 individuals (the minimum number of affected individuals that triggers a mandatory posting on the HHS breach portal). Many now claim United severely underreported the impact and slow-walked information to regulators and the public. By October 2024, just three months later, United confessed that the actual number of affected individuals had grown to 100 million. By January 2025, that number almost doubled to an estimated 190 million individuals – more than half of the U.S. population – becoming the largest known healthcare data breach in American history.

It's believed that the hackers rummaged around Change Healthcare's systems for nine days before they were found out. Once United was clued in, United severed Change Healthcare from the rest of its systems and turned off the lights. As some cybersecurity experts have pointed out, because Change Healthcare did not implement an Endpoint Detection and Response (EDR) tool with ransomware rollback capabilities, which would have maintained frequent, secure back-ups, the com-

pany was unable to restore systems to a pre-attack state. Change Healthcare lost all of its pending claims and transaction data, and was forced to process claims manually. Nearly a month after the breach, United said it would start processing its backlog of medical claims – $14 billion worth. Much of the legal debate in courts now involves how the companies' lack of back-up systems and lack of general preparedness unnecessarily prolonged the harm to everyone downstream.

Providers felt the impact most disparately. The American Medical Association conducted a voluntary survey of providers impacted by the Change Healthcare breach. The study found that 80% of clinicians, most of whom were small practices of 10 physicians or less, lost revenue from unpaid claims. The study also found that 55% of respondents had to use personal funds to cover practice expenses, forcing some practices to cut back on supply ordering, thrusting other practices into payroll penalties, and leading some practices that had been around for years or decades into bankruptcy.

Patients also suffered. The American Hospital Association conducted a similar survey, finding that of 1,000 hospitals surveyed nationwide, 74% reported direct patient care impact, including delays in authorizations for medically necessary care.

Compounding the harm, all covered entities and business associates whose information was included in the breach were required to provide a HIPAA breach notification to both regulators and affected individuals. Breach notices are comprehensive and laborious, particularly for small practices without a back-office staff who can help. They require covered entities to notify affected individuals about the types of information subject to the breach, steps they can take to protect themselves, and curative efforts like what the covered entity is doing to investigate and mitigate the harm, most of which in cases like this are dependent on information released by United and Change Healthcare. Covered entities, like physician practices and hospitals, remained on the hook and faced severe penalties for delay or non-reporting. When United and Change Healthcare slow-walked their disclosures and provided inadequate notice, providers bore the price.

In response to the economic backlash from the breach, United offered affected providers interest free advance payments, or loans, to cover the gap period. In all, United loaned out approximately $9 billion to providers across the country. Providers were led to believe that repayment on the loans was not supposed to occur until the providers determined that "business was back to normal." That did not turn out to be the case.

By October 2024, United reported that it had recouped $3.2 billion in "repayments" and by January 2025 that number grew to $4.5 billion. By April 2025, reports were being made to the media of United's aggressive recoupment efforts, automatically offsetting provider advancements with pending claims and demanding payment of sometimes hundreds of thousands of dollars within days or freezing reimbursements on future claims. The American Medical Association wrote to United urging a flexible approach to repayment and to allow providers some say in how and when to repay the loans based on patient levels, revenue generation, and cost pressures. While United claims to be actively working with providers on flexible repayment plans, the proof is in the pudding. In its revenue report for 2024, United reported revenues of approximately $400 billion, up 8% from 2023, despite the breach.

The legal fall out of the Change Healthcare breach and United's aggressive recoupment efforts has resulted in a flurry of lawsuits. Providers and patients have asserted claims against United and Change Healthcare ranging from the companies' negligence in failing to maintain adequate security safeguards, providing inadequate notices, and violating reimbursement processes and timeliness, to engaging in unfair business practices by employing aggressive recoupment efforts and unfairly passing on the costs of the breach to providers. Lawsuits have been filed by consumers as well as individual providers, practice groups, hospitals, and others.

In an effort by the Courts to streamline the issues and maximize judicial resources, in June 2024, the Judicial Panel on Multi-District Litigation (MDL) determined that a number of lawsuits against Change Healthcare be transferred to the U.S. District Court for the District of Minnesota and coordinated under Judge Donovan Frank.

As of May 2025, there were 78 cases coordinated in the MDL with approximately 26 additional cases filed in various state courts across the country. As the number of lawsuits in state and federal courts continue to rise, Judge Frank issued a letter to state court judges soliciting their input and assistance in coordinating discovery and fact-finding determinations with the lead cases in the MDL. Most recently, in July 2025, two master complaints were filed in the MDL: one on behalf of a class of individuals, and one on behalf of all providers. Providers coordinated in the MDL include those from California, Florida, Illinois, Louisiana, Maine, Massachusetts, Michigan, Minnesota, New Jersey, New York, Ohio, Pennsylvania and Texas. Everyone is getting in line with their pitchforks in hand. Some cybersecurity insurers have also sued United for subrogation, claiming they would not have had to pay their insured's losses if Change Healthcare had implemented proper security measures.

The legislature has taken notice of all the commotion. There have been at least three major legislative proposals resulting from the breach: (1) the Health Infrastructure Security and Accountability Act of 2024 (Senate Bill 5218; introduced September 2024) (which would amend the Social Security Act to require stronger cybersecurity standards and oversight for health information); (2) the Healthcare Cybersecurity Act of 2025 (Senate Bill 1851; introduced May 2025) (which would direct the Cybersecurity and Infrastructure Security Agency (CISA) and Department of Health and Human Services (HHS) to collaborate on cyber threats); and, (3) a HIPAA Security Rule Update (Notice of Proposed Rule Making by HHS; issued December 2024) (which would require stricter requirements for protected health information encryption, network segmentation, and annual risk assessments, with various ancillary risk management measures). None have yet become law, but it is worth pointing out that this is the first time that the Office for Civil Rights has proposed an update to the HIPAA Security Rule in over a decade. Perhaps it is about time.

While the proposed rules facilitate collaboration across agency minds and impose greater accountability on covered entities, only the HIPAA Security Rule update would require that health plans maintain multi-factor authentication and up-to-date secure back-ups in the event of a breach. However, none of the proposed rules require health plans to insure against a potential ransomware attack, nor do they require health plans to indemnify or hold providers harmless for losses or liability resulting from cybersecurity incidents at the health plan level.

Much has been left unsaid about what impact the legal fall-out from the Change Healthcare breach will ultimately have on the U.S. healthcare system and providers when the dust finally settles. Given the losses United faces, it's not likely to go down without a fight. For now, patients who believe their information has been compromised can enroll in complimentary credit monitoring and identity protection services provided through Change Healthcare and can monitor their explanation of benefit forms and bank and credit card statements for suspicious activities. Patients who were denied access to care because of the blackout may have their own claims. Providers who have been impacted by the breach or subjected to aggressive recoupment efforts can review their contracts or seek legal assistance. There are less litigious (and sometimes cheaper) means of resolving payer disputes through internal administrative proceedings. And, it would not be unreasonable for a health plan like United to be open to compromising disputes outside of the public eye to reduce its litigation exposure. If you are thinking about stepping into the ring, put on your gloves, tape up your wrists, and then pull up a chair and wait for that MDL bell to ring.

David A. Rawi *is senior counsel at Lagerlof LLP.*