TESTIMONY OF ADAM BRUGGEMAN, MD, MHA, FAAOS, FAOA

ORTHOPEDIC SURGEON, TEXAS SPINE CENTER

BEFORE THE ENERGY AND COMMERCE COMMITTEE

UNITED STATES HOUSE OF REPRESENTATIVES

REGARDING EXAMINING HEALTH SECTOR CYBERSECURITY IN THE WAKE OF THE CHANGE HEALTHCARE ATTACK

April 16, 2024

Chairman Guthrie, Ranking Member Eshoo, and distinguished members of the Committee, thank you for the opportunity to testify today on this critical topic in our health care system. My name is Dr. Adam Bruggeman, and I am a board-certified orthopaedic spine surgeon from San Antonio, Texas. I am here to share my firsthand experience with the Change Healthcare cyberattack and the impact it has had on my practice beginning in February 2024.

Change Healthcare is a vital component of our health care infrastructure. It serves as a clearinghouse that processes and submits medical claims to insurers on behalf of health care providers. My practice leadership and I were in Washington, D.C., when the attack occurred and, while we did not initially realize the severity, we soon realized its vast implications. We learned that Change would be down for a minimum of four weeks, leaving us unable to process claims and receive payments.

For background, the “life cycle” of patient billing is below:

1. A patient visits a physician for a medical consultation, and the physician documents the encounter and submits charges using appropriate Current Procedural Terminology (CPT) codes (e.g., 99203/99204 for new patients or 99213/99214 for established patients).
2. The billing team reviews the claim for any errors, such as incorrect CPT codes, missing modifiers, or diagnosis codes, before sending it to the insurance payer.
3. The claim is sent to the clearinghouse (Change Healthcare) for additional accuracy checks before being forwarded to the payer.
4. Once the claim passes through the clearinghouse, it reaches the insurance payer for processing and payment.
5. The payer has 45 days to process the clean claim or return it with a denial.
6. Upon processing, the payer sends payment for the service directly to the practice's bank account and an electronic remittance advice (ERA) summarizing the claim, allowable amounts paid, or denials.
7. The practice billing team receives the ERA and posts the payment to the patient's account, reconciling it accordingly. For example, if a practice bills $300 for CPT 99203 and the insurance allowable amount is $150, the insurance company will pay $150, and the practice will write off the remaining $150, leaving a balance of $0 for the patient.

When the cyberattack caused Change Healthcare to shut down, it affected all practices' ability to send claims early in the life cycle and forced physicians to hold claims in the billing bucket until alternative clearinghouse connections were established.

Fortunately, my practice had sufficient cash reserves to continue operating without receiving payments during the outage. This means we did not face the immediate prospect of closing our doors. However, there were still significant challenges. The first was the actual process of submitting claims. We were given the option to switch to an alternative clearinghouse a few weeks into the outage. Unfortunately, not all insurers allowed us to use the alternative for claim submission, as the process of integrating with a new clearinghouse is extensive, costly, and can take months. This made switching impractical. Instead, we had to either hold claims in limbo or resort to submitting them through individual online portals. Although Medicare would have accepted paper claims, our EHR told us it would be 25-30 days before the practice would be approved to submit paper claims. In addition, the EHR was informed that Medicare processing was well behind for paper claims, and it would be at least a 45 day wait before someone could view the claim. For those reasons, we held off submitting any claims while waiting for the system to come back up.

Another major challenge we encountered was the lack of ERAs from insurers, which typically accompany deposits in our bank account and provide critical information about which bills have been paid. Without ERAs, we were unable to reconcile payments with patient accounts, leading to frustrated patients receiving automated bills that should have been marked as paid. My staff had to spend countless hours instructing patients to disregard these erroneous bills.

Even though we have restored access to Blue Cross Blue Shield, Medicare, and TRICARE, the lack of ERAs has not been resolved. Instead, we have been informed that ERAs will not be sent retroactively, and we are having to manually reconcile each deposit by logging into payor websites to obtain explanation of benefits (EOBs) and comparing them to the deposits in our

system. This process takes, at a minimum, 20 minutes per payment and involves accessing each insurance company's web portal to research individual payment amounts then reconcile them with the claim.

Despite broad awareness of the significant challenges so many physicians and other health care providers are experiencing following this cyberattack, insurance companies are—in some cases—rejecting claims due to a lack of timely filing. Imagine a scenario where your billing team, struggling with the aftermath of the cybersecurity attack, finds itself six to eight weeks behind in sending bills. Many insurers enforce a strict three-month timely bill filing requirement, and the Change Healthcare shutdown has effectively crippled your ability to submit claims within this limited timeframe. As a result, when these claims eventually do go through, they are denied on the grounds of untimely filing, forcing the practice to undergo a burdensome appeals process with an uncertain outcome, placing additional stress and financial strain on the already overburdened practice.

The Change outage was disruptive to the business of my practice, but most importantly, it was disruptive to our patients. Every minute my practice administrators spend trying to reconcile ERAs with received payments, assessing which of our patients received incorrect bills, then resubmitting prior authorizations, is time taken away from patient care.

The attack has exposed the vulnerabilities in our health care system and the disproportionate burden placed on physician practices by insurers, government payors, and third-party vendors. For example, our contracts with electronic health record (EHR) vendors suggest that their liability is limited to just three months of payments from our practice to the EHR provider. In the event of a data breach involving even a small number of patients, the costs could easily

exceed this three-month payment threshold. Physician groups are potentially liable for millions of dollars in penalties to patients whose data is stolen. This business practice is unacceptable, as physicians cannot shoulder the entire cost of these failures that were completely outside of our control and that we could not have prevented. We have attempted to negotiate these contract terms with multiple software companies in the past but have been unsuccessful.

My experience is not unique. The American Medical Association recently published the results of an informal survey of 1,400 physicians. Serious disruptions were revealed, with one-third reporting an inability to submit claims, receive payment, or access electronic remittance advice, and 22 percent facing eligibility verification issues which have led to substantial revenue loss. Although Change Healthcare announced it has issued approximately $5.5 billion in support to clinicians and health systems, with simplified terms, these loans have been impractical and many of my colleagues have chosen to forego them altogether. Although this did not happen in our practice, we are aware that some patients across the country had difficulty obtaining medications during this time as well. The outage impacted some pharmacies and their ability to confirm eligibility for coverage of their medications, resulting in patients having to pay full uninsured pricing. We also know that some physicians faced difficulty accessing labs and, most importantly, we still do not know the extent to which patient data was compromised.

As we move forward from this attack, a significant focus will be placed on cybersecurity and data protection, and rightly so. As physicians, we must be able to sit in the room with a patient, document what is happening with their health, and trust that our documentation is safe and secure. We can and must make attacks like this far less likely. However, the role of technology and data in practicing 21st century medicine is only going to continue to grow, making it all but

impossible to build a health care system that is 100 percent impervious to cyber threats. Never again should a single point of failure cascade into a nationwide crisis.

The weaknesses in our health care system that made this attack so far-reaching have been slowly building over many years. If there is one silver lining to this situation, it is that the significant stress on our health care system has shown us where many of these faults lie and the questions we need to answer as we move forward.

First, we need to ask how consolidation and vertical integration are impacting healthcare and may have amplified the impact of this attack. Even on a good day when the system is operating 'normally,' it has been well established that consolidation has not led to improved health of patients and often leads to higher costs.[1] Now we are also seeing how consolidating more of our healthcare spending around a single point of failure can make the situation more severe, more costly, and harder to fix when something goes wrong. As more claims and more patient information continue to be funneled through a handful of large entities, the Federal Trade Commission will also need to look closely at whether vertical integration is making those entities a greater target for cyberattacks.

While Change Healthcare handles an estimated 50 percent of all medical claims and processes more than $1.5 trillion a year in spending, the average physician practice has only weeks to a months' worth of cash on hand in their practice. This makes them especially susceptible and sensitive to cash flow changes, and many have had to go to extreme measures to weather this storm. Fifty-five percent of practices have had to use personal funds to cover their regular

[1] https://www.kff.org/health-costs/issue-brief/what-we-know-about-provider-consolidation/

practice expenses, not to mention the cost of the additional staff time and resources needed to cope with this cyberattack.[2]

Beyond lost revenue, the greatest costs for practices have come from having to find expensive workarounds to process claims, including by entering new, costly arrangements with alternative clearinghouses. As a physician, I do not select the clearinghouse for a given electronic medical record and have no control over how many or which one is selected. Leaving physicians at the mercy of the agreements between EHR vendors and clearinghouses is problematic, especially in the aftermath of this attack where we have seen other clearinghouses take advantage by charging higher prices for setting up "backups." Going forward, we need to investigate whether it is possible to have multiple clearinghouses for a given electronic medical record and build in the redundancies on the front end so that physicians are not left vulnerable.

As this committee is aware, physicians cannot just switch EHRs on a dime if, say, they are unhappy with the vendor's choice of clearinghouse. Aside from the tens if not hundreds of thousands of dollars required to transition from one EHR to another, practices also face significant productivity losses whenever physicians and their staff must learn a new system. This is why it is critical that we build redundancies into the EHR/clearinghouse relationship without adding to the administrative burden of practices.

Once a cyberattack has occurred, especially when payment systems are affected, it is very difficult for physicians to truly be made whole. Advanced payments can help keep practices afloat by covering the delivery of health care services. They do not, however, cover the

[2] https://www.ama-assn.org/system/files/change-healthcare-survey-results.pdf

overtime incurred and extra expense of creating workarounds, pivoting to paper claims, analyzing, and comparing payment gaps, or other issues which cause an incredible amount of extra work for physicians and practice staff. Moreover, conditioning financial lifelines to the usage of workarounds curtails meaningful support for practices in need and denies Change Healthcare's accountability. Furthermore, each insurance company had its own unique process for advanced payments, requiring practices to navigate a complex web of procedures and contact numerous entities to ensure full reimbursement. These companies often limited advanced payments based on the physician's past billing history with them, placing an additional burden on practices already grappling with financial instability due to the cybersecurity breach.

With the desire to continue shifting from fee-for-service arrangements to value-based care, the amount of patient information that physicians will have to track and share among different practices will only increase, leaving patient information even more exposed than it is today. I am concerned that the cost of cybersecurity protection required to accommodate this growth in patient data sharing may serve as yet another barrier for smaller and rural physician groups looking to participate in the movement towards alternative payment models. If these practices are left behind as the rest of medicine moves towards value-based care, they will face even greater pressure to consolidate with larger health systems.

In fact, my concern that cyber threats will drive further consolidation is not just hypothetical. We are already seeing this play out as a direct result of the February attack. For practices whose cashflow was completely cut off and whose cash reserves were spent dry, the financial relief offered by the Centers for Medicare & Medicaid Services (CMS) and Optum, the parent

company of Change Healthcare and a subsidiary of UnitedHealth Group (UHG), was slow to arrive and insufficient. To add insult to injury, some of these practices were purchased by Optum during this situation. There were even reports of Optum using the financial emergency caused by the cyberattack on its own subsidiary as legal justification to expedite its acquisition of physician practices.[3] I find it hard to believe Optum could not have found other ways to support those practices rather than buying them at a discount and consolidating further.

Insurers like UHG have plenty of data to understand their typical charges from and payments to a practice in a typical week. There is little to no reason insurers could not have continued to make weekly payments based on the physician's unique history, then reconciled once the clearinghouse outage was resolved. Recall that insurers are paid premiums in advance of care and had the money on-hand. They just were not releasing that money to physicians due to the inability of physicians to submit bills. Insurers could have significantly helped by pre-releasing the money, then rectifying this on the back end once the claims were able to be submitted instead of burdening the physician's offices with both financial and administrative hardships.

For its part, Congress should clarify the agencies' authority to respond to future disruptions so that impacted parties do not lose precious time waiting for guidance. CMS did not initially indicate that it could financially support physicians through additional payments while waiting for Change Healthcare to get fixed, even though it indicated that it had authority to do so for hospitals. To the extent needed based on legal advice, Congress needs to act to ensure that CMS and the U.S. Department of Health and Human Services is nimble and can quickly deploy

[3] https://prospect.org/health/2024-03-10-unitedhealth-exploits-emergency-change-ransomware-oregon/

financial lifelines to physician practices for any emergency that inhibits cash flows. As noted, many practices have only a few weeks' worth of cash on-hand and the government must be able to support those physicians in times of emergency.

It is imperative that Congress seize this opportunity presented by the recent cybersecurity incident to thoroughly examine whether the growing consolidation within the U.S. health care market truly serves the best interests of patient care. Despite the promised benefits of enhanced productivity and streamlined processes, consolidation has failed to deliver on the lower costs and improved care pledged by the colossal U.S. health care system. In fact, extensive research has consistently demonstrated that increased consolidation has resulted in a pervasive rise in healthcare prices across the board.

The consolidation of practices and their integration with hospital systems has the potential to drive up prices for common orthopaedic procedures, while simultaneously stifling competition and limiting opportunities for independent practices within the same market. To illustrate this point, the costs for knee replacement and lumbar spine fusion procedures were found to be approximately 30 percent higher in concentrated markets compared to those in competitive markets.[4] Expanding the scope further, a comprehensive analysis conducted by the New York Times in 2018 revealed that average hospital prices soar dramatically in the aftermath of mergers. [5] These findings are echoed by numerous other studies, including a 2015 study published in the Journal of the Missouri State Medical Association, which highlighted that hospitals engaging in mergers impose prices that are 40 to 50 percent higher than what they

[4] JC Robinson. Hospital Market Concentration, Pricing, and Profitability In Orthopedic Surgery and Interventional Cardiology. Am J Managed Care 2011; 17(6):e241-e248

[5] https://www.nytimes.com/2018/11/14/health/hospital-mergers-health-care-spending.html

would charge without consolidation.[6] Moreover, a 2015 working paper published by the National Bureau of Economic Research underscores the fact that hospitals without competitors within a 15-mile radius charge prices that are 12 percent higher than those operating in markets with four or more competitors.[7]The trend of consolidation leading to higher costs for patients and payers, while eroding affordability and access to care, demands immediate attention and action from Congress. It is crucial that we critically examine the impact of market consolidation on patient care and take decisive steps to ensure that the interests of patients remain at the forefront of our health care system.

Allowing physicians to practice in the setting that is best for them, their patients and their broader community should be the hallmark of our health care system. Instead, the increase in administrative burden outside of any potential cyberattack makes such events catastrophic for too many providers. I urge the Committee to act and work towards solutions that ensure the stability and security of our health care infrastructure.

Thank you for your attention on this critical matter.

[6] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6170097/
[7] https://www.nber.org/papers/w21815

Summary

My name is Dr. Adam Bruggeman and I am a board-certified orthopaedic spine surgeon from San Antonio, Texas. The Change Healthcare cyberattack, which occurred in February 2024, left my practice unable to process claims and receive payments for a minimum of four weeks. Change Healthcare, a vital clearinghouse in the health care infrastructure, processes and submits medical claims to insurers on behalf of health care providers.

This attack exposed vulnerabilities in the health care system and the disproportionate burden placed on physician practices by insurers, government payors, and third-party vendors. My practice faced challenges in submitting claims, receiving electronic remittance advice (ERA) from insurers, and reconciling payments with patient accounts. This led to frustrated patients receiving erroneous bills and staff spending countless hours manually reconciling payments.

There are significant concerns surrounding the cost of cybersecurity protection required to accommodate the growth in patient data sharing, which may serve as a barrier for smaller and rural physician groups looking to participate in alternative payment models.

Congress should clarify the agencies' authority to respond to future disruptions and ensure that the Centers for Medicare & Medicaid Services (CMS) and the U.S. Department of Health and Human Services can quickly deploy financial lifelines to physician practices in times of emergency. Finally, I urge the Committee to examine the impact of market consolidation on patient care and take steps to ensure that patients' interests remain at the forefront of the health care system.