Statement for the Record: The National Community Pharmacists Association
United States Senate Committee on Finance
Hearing: "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next"

May 1, 2024

Chairman Wyden, Ranking Member Crapo, and members of the committee:

Thank you for conducting this hearing on the cyberattack of Change Healthcare (CHC). NCPA represents America's community pharmacists, including 19,400 independent community pharmacies. Almost half of all community pharmacies provide long-term care services and play a critical role in ensuring patients have immediate access to medications in both community and long-term care (LTC) settings. Together, our members represent a $94 billion healthcare marketplace, employ 230,000 individuals, and provide an expanding set of healthcare services to millions of patients every day. Our members are small business owners who are among America's most accessible healthcare providers. NCPA submits these comments on behalf of concerns we have received from independent and LTC pharmacies.

When the CHC cyberattack occurred on February 2024, parent company UnitedHealth Group (UHG) took the drastic, and appropriate, measure of hitting a "kill switch" to stop the attack's progress. But this immediately disrupted business for all pharmacies with few exceptions because of the vertically integrated nature of UHG.

NCPA believes that UHG has done the bare minimum to help pharmacy providers as we are now over nine weeks from the attack, and independent pharmacies still struggle daily with operational and financial disruptions, including:

Real-time prescription claims processing: Real-time claims adjudication is of the utmost importance for community pharmacies. Pharmacy workflow and recordkeeping are built around it, in contrast to medical, dental, or other providers that invoice patients days or weeks after the provision of care. Prompt reimbursement allows pharmacies to meet payroll, pay wholesaler invoices, and cover other business expenses.

- OptumRx PBM: In its SEC 8-K filing, UHG stated it "believes the network interruption is specific to Change Healthcare systems, and all other systems across [UHG] are operational." However, after the suspected attack was disclosed, pharmacies or their technology partners made the rational decision to disconnect from OptumRx until UHG could prove it had effectively isolated the affected systems. Thus, many pharmacies, even those that connected to OptumRx on a different claims switch, perceived an outage of pharmacy benefit manager (PBM) services. The vast majority of community pharmacies are in an OptumRx network to care for patients with employer-sponsored plans, Health Insurance Marketplace plans, and Medicare Part D plans and in 2023, OptumRx processed 22% of all prescription claims. Implied with real-time claims adjudication is real-time formulary and benefit determination. Without an immediate response from the PBM indicating that a drug was covered for a specific patient on a specific day at a specific

network pharmacy with a specific copay, pharmacies were very concerned about reimbursement for dispensing life-saving drug and future audit liability for nearly a quarter of their business.

- CHC Medicaid fee-for-service processing: The fee-for-service Medicaid program in six states was down, with the last one reported restored over a month after the attack on March 29th. Patients with Medicaid benefits are among the most at risk for poor outcomes when prescriptions and health care are not accessible and affordable.
- CHC claims switch: Pharmacies route drug claims to PBMs in a similar fashion to how a grocery store routes debit card transactions to the card issuer. Pharmacies call this "claims switching" and those that relied on CHC for claims switching were completely cut off from all payers, not just the PBM OptumRx and the six Medicaid programs, for weeks. Some pharmacies were able to start using one of only two competitor switches, RelayHealth or PowerLine, within about a week, but only when their dispensing system technology vendor was able to establish the connection. There are a smaller number of pharmacies that use a dispensing system that is owned in the vertically integrated UHG and could not pivot to a different switch because of how intertwined those systems are. OptumRx should have been more proactive in offering advanced payments to pharmacies unable to transmit claims.
- Financial challenges: The first weekend of the outage, some pharmacies may have been able to rely on pharmacy emergency supply provisions to advance patients a 72-hour supply of medication. If the pharmacy advanced the 72-hour emergency supply at no cost to the patient with the assumption claims processing would be available before that supply ran out, the cost to the pharmacy of advancing the emergency supply depended on the degree to which they relied on various UHG-owned systems and the staggered restoration of those systems. Otherwise, patients were on the hook to pay out-of-pocket for the 72-hour supply of their medications, and as we know some of these systems were unavailable for far longer than 72 hours. If the pharmacy advanced at no cost without being able to submit claims, they probably were at risk of missing wholesaler payments, payroll, rent, etc.

Medicare Part B: Pharmacies also provide for Medicare patients by providing durable medical equipment, supplies, vaccines, and Part B drugs. Many pharmacies rely on a handful of technology solutions to put prescription claims data in a format that is accepted by the Medicare Administrative Contractors (MACs). Pharmacies and other health care providers rely on claims clearinghouses to route claims to the appropriate MAC.

- MedRx and Allwin: CHC operates two businesses, MedRx and Allwin, that provide the service of formatting prescription claims for processing by the MAC, a service critical for pharmacies. As of April 25th, Allwin customers still cannot confirm that backlogged claims from February have been accepted by the MAC.
- Clearinghouse: Pharmacies, among other providers, relied on CHC as a claims clearinghouse. It was not until the week of March 25th that CHC restored this service.
- Claims backlog: the duration of the clearinghouse outage has resulted in an enormous volume of backlogged claims that the MACs need to process and issue payment. In addition to backlogged Medicare claims, pharmacists who have provider status in their state had backlogs of claims to submit to health plans if they were unable to start using a different clearinghouse and/or could not submit claims manually as fast as care was provided.

Copay assistance: Patients rely on copay assistance programs (copay cards, manufacturer copay assistance, copay coupons) to have access to drugs that are not covered by their insurance or are covered but have an unaffordable copay due to the benefit design. CHC administers a range of copay assistance programs and overall did a poor job of communicating the status of these programs. On April 2nd, CHC announced that it transitioned several copay programs to other processors and that progress continues for others.

Payments: On March 29th, CHC disclosed that their finance system for issuing paper checks to pharmacies for reimbursement for certain copay assistance programs was still not restored and pharmacies should enroll for ACH payments. This means that more than a month later, pharmacies still had not received payments, putting their livelihoods and patients at risk if they cannot afford to remain open. **One independent pharmacy regional chain owner told us that they were down 14,600 prescriptions in March from the year prior when before the attack they had been filling prescriptions at a higher rate than in 2023. At this point, they are down over $4 million dollars, with no end in sight. The regional chain has subsequently had to close two locations.**

All-in-all, while shutting down each of CHC's services was necessary, pharmacies were given little to no communication as to what was happening. This impacted not only the CHC switch, but due to vertical integration, nearly every single system that a pharmacy could rely on CHC to do. They were unable to access e-prescriptions, fill prescriptions—particularly prescriptions for controlled substances—or transmit claims. They had no way of knowing if a patient's plan would cover the drugs they were filling or if they would be paid back for them, and at times this meant asking their patients cover the costs of the drugs out of pocket. UHG should have to answer for the fact that there was no backup. It continued to collect premiums and did the bare minimum to help independent pharmacies that, along with their patients, are still grappling with the aftereffects nearly two months later, as some systems are still not online.

Additionally, PBMs are beginning to issue audits into prescriptions dispensed in the aftermath of the cyberattack. PBMs are telling pharmacies that they need to comply with the rules surrounding government health programs, while at the time pharmacies filled prescriptions in good faith to patients so as to not impact their health negatively. While OptumRx modified its audit program to exclude prescriptions dispensed during the outage, others have not. This comes at a time where pharmacies are already on the brink of closure, and with this additional strain it may prove too much, accelerating the loss of pharmacies and patient access to care.

Pharmacies and their patients deserve better, as such NCPA looks forward to working with Congress as you look to find answers, hold those responsible accountable, and provide relief to those impacted. Thank you for your attention to this matter.

To this end, we ask that Congress to:

- Ask HHS to revise 42 C.F.R. § 423.505(p)(1)(B) (contract provisions in Part D regulations) to:

  - Include language that PDPs (and their subcontractors, such as PBMs) must communicate with pharmacies and other partners in the provider network within 24 hours of notification of a cyberattack and every 24 hours until essential functions are restored.
  - Require PDPs to have their contingency plans posted on their public website, and in the event of a disaster/cyberattack, post the contingency plan and information about restoration of essential functions on their main home page (or linked to on home page).
- **Establish HHS crisis communications plans for future attacks:** Although Change Health and its Optum/United Health Group leadership were in almost immediate contact with customers, HHS did not engage fully until several days after the issue arose and after many of the undersigned organizations sent inquiries. In future event, HHS should be acting as an immediate conduit for information, particularly for those people who are not included in the vendor-hosted calls or emails.
- **Direct Plans and PBMs to Pause Audits:** Future attacks should prompt an immediate pause of audits until services are restored. Although Optum has indicated that it took this step, other payors did not and although HHS indicated it requested other payors take this step, there has been no public response from those payors as to how they will handle the period of outage during audits.
- **Make Pharmacies Whole for Good Faith Dispensing**: Identify payment solution that will make pharmacies whole for medications dispensed, and cost-sharing collected, based on good faith efforts to ensure continuity of patient care during this cyberattack.
  - Revise § 423.750 (regarding intermediate sanctions and civil monetary penalties under Medicare Part D) to:
    - Establish a Pharmacy/Provider Recovery Fund.

      This fund could collect penalties to create a fund available to pay for costs incurred by pharmacy and other providers due to cyber-created or disaster-related outages. This fund would allow providers to continue to provide services, particularly for new patients waiting for authorization The fund would cover additional costs incurred by pharmacies and providers including extra staff costs due to PDP and PDP contractor (such as PBM) contingency plans. Similar funds that have been created by legislation include the CFPB Civil Penalty Fund (https://www.consumerfinance.gov/enforcement/payments-harmed-consumers/civil-penalty-fund/) and the HRSA Provider Relief Fund (https://www.hrsa.gov/provider-relief)
- **Prevent Punitive Payer Actions**: Prohibit payers and PBMs from imposing DIR fees based on disruptions in care or recordkeeping that resulted from the cyberattack.
- **Address Longer-Term Impacts**: Urge HHS to clarify that providers will be held harmless for any data breaches attributable to the Change Healthcare cyberattack. Given the reports of a second breach of the Change system focused on patient data, providers remain concerned that patient data could have been breached without their knowledge.

Conclusion

The above examples demonstrate the financial hardship and substantial healthcare risks that patients experienced due to the CHC cyberattack. This reinforces the importance of cybersecurity measures in

healthcare systems to ensure continuous access to necessary medications; patients should never have to choose between their health and financial strain due to their insurers' cybersecurity issues. The examples above also demonstrate how community pharmacies continue to be disadvantaged by the cybersecurity attack. We urge Congress to act urgently to prevent these types of consequences from occurring in the future.