March 1, 2024

The Honorable Xavier Becerra
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, DC 20201

RE: Change Healthcare Cyberattack Impact on Patient Care

Dear Secretary Becerra:

On behalf of our more than 60,000 pharmacists, student pharmacists, and pharmacy technician members practicing across all patient care settings, we are requesting that the U.S. Department of Health and Human Services (HHS) take additional action in response to the ongoing cyberattack on Change Healthcare.

ASHP appreciates HHS's engagement as providers and patients navigate this unprecedented cyberattack. The impact on our members, and consequently, their patients, cannot be understated. Many hospital and health-system pharmacies have reported being unable to process pharmacy claims or access e-prescribing. To work around these limitations, providers have been forced to move to new systems or default to paper recordkeeping, significantly increasing workloads, slowing workflows, and creating compliance concerns. For patients, the cyberattack has meant delayed prescriptions, and the choice between paying full price for a prescription (which can mean hundreds or thousands of dollars out of pocket) or going without until the attack is resolved and normal processing resumes.

We recognize that responsibility for restoration of service lies with Change Healthcare, but considering the depth and breadth of the impact, we urge HHS to take certain actions to assist providers until the crisis is resolved. Specifically, HHS should:

- Increase Provider Communications: Although Change Healthcare has been in contact with providers through calls facilitated by UnitedHealth Group, our members are still struggling to get information about the timeline for service restoration and reassurance that prescriptions that are filled while services are down will be reimbursed. We urge HHS to act as a conduit for updates from Change Healthcare, sending them out via established HHS communications channels.

- Direct Plans and PBMs to Pause Audits: Audits should be paused during the cyberattack. Through no fault of their own, pharmacies and other providers have been placed in a position of scrambling to maintain patient services. Health plans and PBMs should be directed to pause audits or compliance reviews until the cyberattack has been resolved.

- Provide Regulatory Flexibility: Until services are restored, we urge HHS to provide flexibility and/or to exercise enforcement discretion related to e-prescribing and "good faith" estimates of costs for prescriptions.

- 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.

- 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: Although providers are currently focused on addressing pressing needs, they remain concerned about potential long-term fallout. Specifically, we urge HHS to clarify that providers will be held harmless for any data breaches attributable to the Change Healthcare cyberattack. Further, HHS should ensure that, for the purposes of audits and surveys, the period of the cyberattack is treated with leniency, to ensure that providers are not punished for lapses that were no fault of their own.

Finally, we urge HHS to take steps to create a national action plan for future cyberattacks. Specifically, the agency should consider convening stakeholders to outline response plans, including communication plans for providers and the public, to reduce confusion and minimize impact on patient care.

We appreciate HHS's efforts to assist providers during the cyberattack. ASHP stands ready to provide any assistance we can offer as efforts to resolve the cyberattack continue. Please do not hesitate to reach out with questions or requests for additional information about the cyberattack's impact on our members and the patients they serve.

Sincerely,

Tom Kraus, J.D.
Vice President, Government Relations