

Congress of the United States

Washington, DC 20515

[[DATE]]

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

Dear Secretary Becerra:

We write regarding the cybersecurity attack on Change Healthcare and the resulting disruptions that have affected patients, physicians, other health care providers, and the smooth operations of the nation's healthcare system.

We appreciate the Department of Health and Human Services' (HHS) announcement about assistance to hospitals dated March 5, 2024, and physicians dated March 9, 2024. We urge HHS to follow up on these announcements by using all its authorities to ensure timely payment across the board in Parts A, B, and C of Medicare.¹² Additionally, we ask for HHS to work with states to ensure Medicaid and the Children's Health Insurance Program (CHIP) are able to receive timely payments so that all aspects of the health care system can continue to remain open, fully functional, and accessible to patients. We appreciate the acknowledgement dated March 6, 2024, of the impact this attack has had on physicians and other providers and urge you to keep us informed.³ We also ask that HHS take steps to address the inability of many patients to receive timely access to medications, given disruptions in verifying patients' identities and eligibility for coverage due to the Change Healthcare cyberattack.

We underscore that we are not requesting new taxpayer money into the health care system. Rather, we request that HHS use its existing authorities to ensure that money that should be flowing for services rendered under traditional Medicare and Medicare Advantage, and under Medicaid, continues to do so. Just as with hospitals anticipating Part A payments, multiple physician practices anticipating payment for Part B services rendered have seen their cash flow radically impaired given disruptions in clearinghouse operations and the impact on payers, including health plans participating in Part C.

Smaller physician practices already operate under slim financial margins, especially with the recent cuts in Medicare reimbursement. These challenges are also more acutely felt by practices in rural and underserved areas. While smaller practices potentially face possible closure, larger practices still face an inability to meet payroll. Additionally, while problems stemming from the Change Healthcare attack are not universal throughout the U.S. healthcare system, they are extremely dire for the practices and organizations that have been affected. Examples include billing and cash flow disruptions, prior authorization transmission delays, and remittance issues for

¹ <https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html>

² <https://www.cms.gov/newsroom/fact-sheets/change-healthcare/optum-payment-disruption-chopd-accelerated-payments-part-providers-and-advance>

³ <https://www.cms.gov/newsroom/press-releases/cms-statement-change-healthcare-cyberattack>

electronic prescriptions. If the department needs flexibilities granted in law, please let us know so we can work together to ensure patient access and care are not negatively impacted.

For non-Medicare-related payments, we also ask that HHS continue its discussions with United Health Group, Optum, and Change Healthcare to provide financial and other assistance to affected healthcare organizations. We understand from providers that the assistance provided to date by UHG/Optum/Change does not fully mitigate the financial harm caused by the suspended and delayed payments from commercial insurers.

Additionally, we are concerned about the impact of this cyberattack on patients. Recent articles have detailed patients who must cover the entire cost of their medications, or even go without, when pharmacies are not able to find workarounds for the lack of access to insurance coverage information.⁴ Furthermore, our offices have received concerns from constituents who have paid out-of-pocket for their medical supplies with no known solution for how to make them whole. We are worried about our constituents' ability to afford these expenses. In this current incident, individuals who have been forced to cover the costs of their medications and care out-of-pocket, particularly those on fixed incomes or reliant on high-cost medications, may encounter challenges in paying other bills in the coming weeks. Moreover, the exposure of personal and protected health information to other cybercriminals poses a lasting threat, increasing the risk of identity theft and targeted scams. This is particularly concerning for older Americans who are at an elevated risk of being targeted and becoming victims of financial scams and fraud. As the Administration is called upon to aid the various impacted parties affected by the attack, we request timely responses from the Administration to the following questions:

1. Does CMS have the statutory or regulatory authority to provide Part B physicians and other health care providers that receive Advance Payments more flexible repayment terms?
2. Has the administration received concerns regarding patients having to pay out of pocket for medical services or medications?
3. Due to the high probability that sensitive information was compromised during this incident, can the Administration provide guidance on how Change Healthcare should proceed to ensure that patients are safeguarded against malicious actors?

Thank you for your timely attention to this request, at a moment of real crisis for a portion of our nation's healthcare system.

[[CLOSING]]

[[SIGNATURES]]

⁴ <https://www.cybersecuritydive.com/news/change-healthcare-providers-impact/709236/>;
<https://www.nbcnews.com/health/health-care/cyberattack-change-healthcare-patients-struggle-get-medication-rcna141841>