



May 1, 2024

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

Dear Secretary Becerra:

On behalf of the American College of Physicians (ACP), I am writing to express our continued concerns regarding the recent cybersecurity incident involving Change Healthcare and its significant and ongoing impact on physicians. The College is the largest medical specialty organization and the second-largest physician group in the United States. ACP members include 161,000 internal medicine physicians, related subspecialists, and medical students. Internal medicine physicians are specialists who apply scientific knowledge and clinical expertise to the diagnosis, treatment, and compassionate care of adults across the spectrum from health to complex illness.

In March, ACP wrote a letter [to HHS](#) highlighting the significant financial strain this cyberattack has imposed on physicians who rely on Change Healthcare's claims and billing systems, the largest in the U.S. health care system. Unfortunately, in the past month, physicians, especially those in smaller practices that serve rural and underserved communities, have continued to have cash flow issues that severely threaten patient access to care and practice viability.

UnitedHealth Group and Change Healthcare have not done enough to support and resource physicians over the past two months. Instead, many physicians have been without the necessary capital to provide care since the cyberattack, and most practices are unaware of the steps that HHS and others have taken to establish workarounds. A [recent survey](#) from the American Medical Association found that in the aftermath of this cyberattack, 55% of practices have had to use personal funds to cover expenses, and about one-quarter of practices have received financial assistance from UnitedHealth Group. **The College is therefore strongly urging that HHS take further action to work with UnitedHealth Group, Change Healthcare, and other necessary actors to ensure these measures are communicated and implemented consistently and expeditiously.** ACP is deeply concerned that absent these actions from HHS, physician practices will be forced to drastically scale back patient panels, restrict the type of care provided, explore alternative financing options, or close their practice altogether.

After the cyberattack forced Change Healthcare to halt its functionality as a clearinghouse for billing and reporting, the flow of payments to physicians was severely disrupted. One of the solutions proposed by UnitedHealth Group and Change Healthcare was for physicians to switch to other clearinghouses to receive their payments. However, this is not a practical solution for many physicians due to the significant barriers that make switching clearinghouses burdensome. Since this cyberattack, other

clearinghouses have significantly increased their transfer costs, and physicians have also encountered difficulties integrating these clearinghouses into their existing electronic health record (EHR) systems. At the same time, physicians and health plans are understandably hesitant to reconnect to Change Healthcare's systems after the cyberattack due to a lack of trust, further exacerbating the situation.

ACP believes that HHS must continue to alleviate the burden on physicians and provide short-term relief. First, we understand physicians in smaller and more rural practices have not received adequate messaging on the cyberattack and follow-up actions. **We recommend that HHS take additional action through direct mailings, phone calls, and fax messages to communicate with smaller and more rural practices.** Many of the resources and information that HHS has shared have been incredibly valuable, and we want to ensure that all physicians are aware of these resources. ACP strongly recommends that HHS work with national and state medical societies and partners to ensure that physicians promptly receive and can inquire about these resources. Smaller and more rural practices often do not have access to the same resources as larger health systems. HHS must leverage the connection between physicians, medical societies, and partners to distribute resources and other information more effectively.

Last month, CMS extended the data submission deadline and reopened the 2023 Merit-based Incentive Payment System (MIPS) Extreme and Uncontrollable Circumstances (EUC) Exception Application to provide relief to eligible physicians and other clinicians impacted by the Change Healthcare cybersecurity incident. Extending these deadlines into April was essential for eligible physicians, and **we strongly urge HHS to ensure that impacted physicians in MIPS are not unfairly penalized throughout this entire performance year.** Even though Change Healthcare's systems are gradually returning to operational status, system outages have persisted for two months, and some systems still are not fully restored. Physicians will feel the effects of this for many months to come.

We also recommend that HHS take steps to allow and encourage paper claims for an extended grace period following the complete restoration of Change Healthcare's systems. Currently, practices are backlogged on administrative tasks and claims submissions and are also facing the choice of reconnecting to the Change Healthcare systems or choosing a new clearinghouse. As previously stated, there is a learning curve for physicians when adopting these new clearinghouses, and physicians should not be forced to choose between providing care and completing administrative tasks disrupted by this incident. Allowing paper claim submission during this transition period and for months after would allow physicians to place their primary focus on clinical practice. ACP recommends extending this grace period to 90 days after completely restoring all of Change Healthcare's systems.

ACP further recommends that HHS and state Medicaid plans provide flexibility and allocate funds to minimize the stress placed on physicians. HHS' encouragement of these state-based actions is critical to reaching the most marginalized patients and the physicians who care for them. HHS should also encourage UnitedHealth Group to adjust its allocation period to 60 days instead of the current 30 days. This allows physicians a longer period to provide care, perform necessary administrative tasks, and



determine if additional allocations are needed. The repayment timeframes are also problematic as most physicians will not have adequate cash flow to return payments within 30 days after standard operations resume. Health plans should be aware of these cash flow disruptions, and their flexibility during this time is essential to getting physicians back on schedule. **Additionally, ACP recommends supplemental advanced payments to physicians through traditional Medicare and private payers.** The current payments primarily address providing direct patient care, but practices routinely incur costs for clinical staff, resources, and other expenses. The lack of these actions and delays in reimbursement will lead to a significant decrease in the number of physicians able to provide care, elimination of staff, and use of personal funds to keep practices operational.

In addition to the continued concerns about cashflow disruptions and access to care, ACP is incredibly disturbed by reports that UnitedHealth Group has used this recent cyberattack to take advantage of practices that are struggling financially by buying them out and expediting mergers with UnitedHealth Group. Due to the attack against its systems, practices have been financially distressed. ACP believes it is a predatory practice for UnitedHealth Group to acquire practices vulnerable to its own cyberattack. **We urge HHS to investigate these predatory practices** and take any corrective or adverse action where appropriate. HHS should also leverage its partnerships with states as additional agencies begin to examine UnitedHealth Group's behavior.

As HHS continues to work with physician partners, Change Healthcare, and UnitedHealth Group to address these issues, **ACP strongly encourages special attention to be paid to the ongoing and rising cybersecurity and privacy risks within the healthcare infrastructure.** HHS and federal agencies responsible for protecting and securing health data must guarantee that these delays, barriers, and breaches are not repeated in future cyberattacks. These gaps must be addressed in future rulemaking, and appropriate penalties must be assessed due to any adverse findings via investigation.

ACP has appreciated the work of the Department to support physicians and patients over the past two months. The College will continue to give feedback to HHS and inform our members' perspectives during this challenging time. We look forward to a continued partnership with HHS now and in the future, as physicians continue to feel the effects of this cyberattack. Please contact Dejaih Johnson, JD, MPA, Manager, Regulatory Affairs for the American College of Physicians, at djohnson@acponline.org or (202) 261-4506 with questions or comments about the contents of this letter.

Sincerely,

A handwritten signature in blue ink that reads 'Leslie F. Algase MD, FACP'.

Leslie F. Algase, MD, FACP
Chair, Medical Practice and Quality Committee
American College of Physicians