

HHS letter regarding the Change Healthcare cyber attack

07/24/2024 3:10 pm EDT

Attached please find a link to a letter dated March 25, 2024.

<https://healthsectorcouncil.org/wp-content/uploads/2024/03/HHS-Letter-and-Appendix-to-HC-Providers-1.pdf>



March 25, 2024

To the healthcare provider community:

As many of you have experienced, the impacts of the cyberattack against Change Healthcare have continued to disrupt provider billing and claims operations. At the U.S. Department of Health and Human Services (HHS), the Administration for Strategic Preparedness and Response (ASPR), and the Centers for Medicare & Medicaid Services (CMS), we have heard concerns from so many providers - from pediatricians and ophthalmologists to infusion centers, home- and community-based services providers, and community health centers - about cash flow disruptions in the aftermath of the Change Healthcare cyberattack.

The Biden-Harris Administration is leading with solutions, providing flexibility for state Medicaid programs to provide interim payments to fee-for-service providers, making advance and accelerated payments available to providers and hospitals through Medicare, and urging health plans to do the same. We continue to press UnitedHealth Group and private healthcare plans to follow our lead.


We also continue to hear from providers that you have sometimes had difficulty getting answers from healthcare plans about the availability of prospective payments or the flexibilities you may need while the Change Healthcare platform is unavailable. HHS asked health plans to provide specific national contact information that providers can use when they need this information, and we are providing that information to you enclosed with this letter. Please share this resource with providers who need it. However, if you have a regional point of contact for your health plan, we'd suggest you reach out to them first. If you reach out to these contacts and do not receive a response, please contact us at HHScyber@hhs.gov.

We also encourage you to review and implement HHS's voluntary Healthcare and Public Health Cybersecurity Performance Goals (<https://hphcyber.hhs.gov/performance-goals.html>), which are designed to help healthcare organizations strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety.

We appreciate your resilience and your continued commitment to your patients during the last month. And thank you for remaining engaged with us to make sure we know about the challenges you have faced in light of the Change Healthcare cyberattack. It has been helpful for us to hear directly from you to understand the scope of those challenges and to know how to tailor our response to your needs. We will continue to value your feedback as we move forward together.



Andrea Palm
Deputy Secretary



Dawn O'Connell
Administrator and Assistant Secretary, ASPR



Chiquita Brooks-LaSure
Administrator, CMS

Enclosure