



March 7, 2024

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

Subject: Change Healthcare Outage's Effects on Aging Services Providers

Dear Secretary Becerra,

On behalf of our more than 5,400 nonprofit and mission-driven aging services providers from across the continuum of aging services and our 36 state partners in 41 states, LeadingAge appreciates the Department of Health and Human Services (HHS) diligent, coordinated response and activities related to the cyberattack affecting Change Healthcare. Our aging services providers continue to be impacted by delays in claims submission and timely filing requirements, with providers forced to use time-consuming workarounds that require manual processes that are not sustainable.

Additionally, the solutions and funding options offered thus far by Optum are not clearly available to our provider segment as many of our members use a third-party vendor who in turn used Change Healthcare as a clearinghouse. Due to the layers of vendors, many of our members were caught off guard by the interruption. Delays in payment could continue for weeks or months before resolution. Aging services provider margins are already tight and aging service providers do not typically have the same reserves as hospitals or physician groups to weather this kind of disruption.

We understand the payment system for hospitals has been significantly impacted due to the daily rates paid to those providers. However, our post-acute, long-term services and supports (LTSS) and hospice providers may see a delayed impact as they are just now billing for February services. For this reason, we do not yet know the full magnitude of the financial impact of the Change Healthcare outages on their organizations. We want to underscore the critical importance and interconnectedness of these providers in the broader health care continuum. More than 40% of hospitalized Medicare patients receive post-acute services after discharge, mostly in the home with home health or in a skilled nursing facility. Furthermore, many more unaccounted transfers occur for acute care to hospice. Nursing home revenues are at financial risk on both the Medicare and Medicaid side from the Change Healthcare cyberattack placing frail older adults' care in the balance while they scramble to adopt workarounds, submit manual claims and/or change clearinghouses.

Beyond the short-term cash flow concerns, the disruption to claims submission has broader implications for the quality measures that are generated from this data. In particular, each of these settings has claims-based quality metrics used to calculate their performance on rehospitalizations, emergency department usage, and overall healthcare spending through their respective quality reporting programs and/or value-based purchasing programs. Post-acute care provider payments are at risk of having their annual payments reduced by 2-4% because the claims data cannot be adequately reported due to this disruption.

We therefore request HHS and CMS take the following actions to protect America's aging services providers:

- CMS should encourage Medicare Advantage plans as well as Medicaid and CHIP Managed Care Plans to be prepared to accept paper claims from providers who need to file them.
- CMS should encourage Medicare Administrative Contractors, Medicare Advantage, Medicaid, and CHIP managed care plans to issue paper checks on timelines comparable to electronic payment, where there is interruption in the payment process.
- CMS should encourage Medicare Advantage plans as well as Medicaid and CHIP Managed Care Plans to offer advance funding to providers most affected by this cyberattack and follow a similar process to the Medicare Financial Management Manual, Chapter 3, Section 150, including consistent payment calculations, recoupment timelines, and no additional fees;
- CMS should review impacts on claims-based measure calculations for all settings' Quality Reporting Programs, value-based care programs, and Care Compare refreshes. If CMS identifies any adverse impacts, reporting of these measures should be delayed allowing time for providers to ensure claims were properly processed and the resulting quality measure data was not impacted;
- CMS should outline the expected impacts on value-based care programs (home health value-based purchasing expansion and skilled nursing value-based purchasing) and reimbursement structures to minimize adverse impacts to participating providers;
- CMS should advise State Health Departments, Survey Agencies, and Accrediting Organizations of the operational and financial challenges associated with this event to contextualize grievances from beneficiaries and reduce unnecessary citations or complaint surveys related to factors outside of the direct control of home health agencies, hospices, and skilled nursing facilities, and Medicaid home and community-based services (HCBS) providers; and
- HHS should develop consumer facing information regarding this attack for providers to properly explain the potential impacts to care directing consumers to the appropriate complaint channels about the impact on care.

As these cyberattacks continue to increase, we see the omission of post-acute, long-term care and hospice providers in *Healthcare Sector Cybersecurity: Introduction to the Strategy of the U.S. Department of Health and Human Services* as erroneous and short-sighted. We strongly encourage HHS and CMS to take the following actions to protect beneficiaries who utilize post-acute care and Medicaid funded LTSS in the face of growing cybersecurity threats:

- HHS should include post-acute, long-term care and hospice providers in further development of cyber security strategies for the entire health care industry;
- In any new authority and funding obtained by HHS through congressional action to administer financial support and incentives to implement high-impact cybersecurity practices should include post-acute, long-term care and hospice providers;

- CMS should clearly outline the provider liability when choosing third party claims processing services and those entities should be responsible for disclosing if they use another clearinghouse or third party administrator; and
- HHS should clearly outline the party responsible for HIPAA accountability and their communications responsibility in the event of a cyberattack affecting multiple downstream providers.

We are grateful to HHS and CMS for their partnership in protecting vulnerable patient data. LeadingAge stands ready to collaborate to develop solutions. We are available to discuss these or other issues. Please contact Linda Couch, Senior Vice President of Policy and Advocacy, at [louch@leadingage.org](mailto:louch@leadingage.org) with any questions or to follow up with the LeadingAge team.

Sincerely,



Katie Smith Sloan  
President and CEO, LeadingAge

CC: Chiquita Brooks-LaSure, Administrator, Centers for Medicare and Medicaid Services  
Dr. Meena Seshamani, MD, Ph.D., Deputy Administrator and Director, Center for Medicare, Centers for Medicare and Medicaid Services  
Daniel Tsai, Deputy Administrator & Director, Center for Medicaid & CHIP Services, Centers for Medicare and Medicaid Services