DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C4-21-26
Baltimore, Maryland 21244-1850

CENTER FOR MEDICARE

April 9, 2024

Mr. Thomas Ryan
President & CEO
American Association for Homecare
1400 Crystal Drive, Suite 460
Arlington, VA 22202

Dear Thomas Ryan:

Thank you for your letter outlining your concerns regarding the recent cyberattack on Change Healthcare and its impact on Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) suppliers and the Medicare beneficiaries who rely on these products. The Centers for Medicare & Medicaid Services (CMS), together with its government partners, is closely monitoring this cyberattack to assess the impact on access to care. We understand the significant and immediate impact that this cyberattack has had on all facets of the health care industry, including those involved in supplying medically necessary DMEPOS items and services to patients in their homes.

In response to this cyberattack and the disruptions it has caused, CMS has provided flexibility for state Medicaid programs to provide interim payments to fee-for-service providers,[1] and made accelerated payments available to providers and suppliers respectively through Medicare.[2] CMS has also urged health plans, including Medicare Advantage plans, Medicare Part D plans, Medicaid and CHIP managed care plans, and private insurance to consider offering advance funding to providers and suppliers.[3]

CMS also published a Health Plan Management System (HPMS) memo on March 6, 2024, titled, "Addressing Impacts Related to the Cyberattack on Change Healthcare."[4] The memo outlines guidance for the actions MA organizations are encouraged to undertake as a means of mitigating the impact on downstream entities such as health care providers and suppliers. The memo also states, in part, that "we encourage MA organizations to remove or relax claim filing deadlines

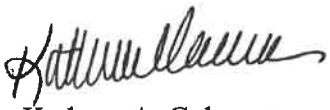
[1] https://www.medicaid.gov/sites/default/files/2024-03/cib031524.pdf
[2] https://www.cms.gov/newsroom/fact-sheets/change-healthcare/optum-payment-disruption-chopd-accelerated-payments-part-providers-and-advance
[3] https://www.hhs.gov/about/news/2024/03/05/hhs-statement-regarding-the-cyberattack-on-change-healthcare.html
[4] https://www.cms.gov/about-cms/information-systems/hpms/hpms-memos-archive-weekly/hpms-memos-wk-2-march-4-8

and requirements to provide additional flexibility to providers as the normal claim submission process may be disrupted by this event." We further indicated that "[w]e encourage MA organizations to offer advance funding to providers most affected by this cyberattack." Finally, CMS emphasized the requirements under 42 C.F.R. § 422.504(o)(1) and § 423.505(p)(1), which require MA organizations and Part D sponsors to develop, maintain, and implement business continuity plans to ensure restoration of business operations following disruptions.

Additionally, on March 25, 2024, CMS provided additional guidance to impacted health care providers and suppliers in a document titled Resources for Providers in Response to the Change Healthcare Cyberattack. The attached document is a compilation of information, resources and tools from health plans and payers for providers in need of assistance. In the document, providers will find information to help them connect with payers regarding impacts of the cyberattack, links to resources payers have set up (including guides to connect to alternate data clearinghouse services), information on advance payments, and more.

We appreciate your feedback as we navigate this difficult situation. Additional comments or requests regarding the impact of this situation may be directed to our policy mailbox at https://dpap.lmi.org/dpapmailbox/mailbox.

Sincerely,



Kathryn A. Coleman
Director
Medicare Drug & Health Plan Contract Administration Group

Attachments