

## Cybersecurity Alert: Change Healthcare

### Federal Relief Efforts to Date and AHCA/NCAL's Request for Audit Relief

As we informed you last [week](#), on February 21, 2024, UnitedHealth Group Inc.'s technology subsidiary Change Healthcare announced that its systems were adversely affected by a security incident. At that time, we offered [suggestions](#) for providers to contact their claims processing technology vendors and payers for updates to determine if they were impacted, provided strategies to consider using existing processes for requesting Medicare accelerated payments, and we [submitted a letter](#) to the U.S. Department of Health and Human Services (HHS) Secretary Xavier Becerra requesting that HHS and the Centers for Medicare and Medicaid Services (CMS) take specific actions in response to this issue.

Over the past two weeks, we have learned more about the breadth of the impact on long term and post-acute care community as most claims submissions and billing activities occur at month-end. Initially, it appeared that the risk for providers encountering claim processing activities and receiving payment was limited to providers who use software vendors integrated with Change Healthcare clearinghouse services. Since then, it's been discovered that many payers, including some Medicare Advantage (MA) plans, some State Medicaid systems, and commercial payer claims processing and payment systems that also utilized Change Healthcare systems for certain activities could result in disruption of provider payments.

#### Provider Relief Options to Date

On Friday, March 1, UnitedHealth Group announced a very limited [temporary funding assistance program](#) through Optum Financial Services, **but only for providers whose payments are issued through Change Health systems.** However, our analysis indicates that this limited assistance would not help most impacted AHCA/NCAL member providers.

Yesterday (March 5), [HHS announced](#) steps that CMS is taking to assist providers affected by this situation to continue to serve patients. Many of these steps were requested by AHCA/NCAL in our [letter to HHS last week](#). Per HHS, CMS will

---

continue to communicate with the health care community and assist, as appropriate. Providers should continue to work with all their payers for the latest updates on how to receive timely payments.

The [HHS announcement](#) also discusses the right for providers to submit a request for an accelerated payment if they experience significant cash flow problems from the unusual circumstances impacting their operations. **While the HHS announcement singled out hospitals as an example, the accelerated payment option is also available for SNF providers** as described in [our update last week](#). During outages arising from this event, facilities may submit accelerated payment requests to their respective servicing Medicare Administrative Contractor (MACs) for individual consideration. HHS is working to provide additional guidance to the MACs about the specific items and information a provider's request should contain, and information will be available from the MACs later this week.

AHCA/NCAL also suggests that impacted providers submit an accelerated payment request to their MAC **with supporting documentation**, including messages from their billing vendor, payer, or other health information technology partner that say providers may/will have payments delayed or will have to perform workaround activities to complete those workflow functions disrupted by the Change Healthcare cybersecurity breach. Screenshots of billing software dashboard notifications/error messages indicating that certain claims processing transactions cannot be completed through the normal pathways may also be helpful.

### **Additional AHCA/NCAL Request for Audit Relief**

Many AHCA/NCAL members have reassigned numerous personnel or have needed to hire additional temporary personnel to manually process claims for multiple federal, state, and commercial payers, including MA plans, using available workarounds. Notably, these are often the same individuals involved in responding to the claim additional documentation requests (ADR) issued by CMS contractors as part of the Agency's program integrity medical review processes.

This has created a perfect storm for those providers whose claims processing operations have been adversely impacted by the Change Healthcare cybersecurity crisis. **Earlier today, AHCA/NCAL submitted a [follow-up letter to HHS Secretary Becerra](#) requesting that CMS extend temporary pre- and post-pay audit flexibility to 90 days for LTPAC providers who attest their claims processing operations related to any payer are affected by the Change Healthcare cybersecurity incident and ongoing systems outage.** We're also asking HHS to encourage Medicare Advantage (MA) Plans and State Medicaid Agencies to consider offering similar audit flexibilities for providers

---

affected by the Change Healthcare cybersecurity crisis. This is an evolving situation, but we recognize how critical this is to our impacted members.

This is an evolving situation, but we recognize how critical this is to our impacted members. We will continue to keep you apprised of any developments or share any guidance through this situation.

Please contact [Grant Beebe](#) or [Dan Ciolek](#) at AHCA/NCAL with any questions.

---

*This message contains confidential information and is intended only for AHCA/NCAL membership. Dissemination, distribution or copying the contents of this email beyond this group is strictly prohibited.*



---

[AHCA](#) | [NCAL](#) | [Provider](#)