Change Healthcare cyberattack

In the wake of the massive impact the Change Healthcare cyberattack is having on physician practices, the AMA is advocating at all levels to find workable solutions to allow practices to maintain financial stability and continue providing timely patient care.

Life after Change Healthcare cyberattack: Without payment for claims, physicians struggle to keep practices afloat

Survey results from the AMA demonstrate that the economic harm to practices and patient-care impact of the Change Healthcare cyberattacks are ongoing. The AMA conducted two recent informal surveys that show the continuing, devastating impact of the Change Healthcare cyberattack, which threatens the viability of physician practices across the country, and according to respondents, has serious implications for patient care.

According to our most recent survey released on April 29 (PDF), respondents report continuing issues with multiple operations, despite UnitedHealth Group's announcements of restored service: 60% continue to face challenges in verifying patient eligibility; 75% still face barriers with claim submission; 79% still cannot receive electronic remittance advice; and 85% continue to experience disruptions in claim payments.

This new survey builds upon our previous survey results released on April 10 (PDF), that indicated service disruptions from the cyberattack have led to severe consequences for physician practices**:** 80% have lost revenue from unpaid claims; 85% have had to commit additional staff time/resources to complete revenue cycle tasks; and 78% have lost revenue from claims that they have been unable to submit. It is also important to note that restricted functionality since the cyberattack has resulted in: 36% of respondents reporting suspension in claim payment; 32% being unable to submit claims; and 22% being unable to verify eligibility for benefits. Practices of 10 or fewer physicians appear to be particularly hard hit.

"The disruption caused by this cyber-attack is causing tremendous financial strain," said AMA President Jesse M. Ehrenfeld, MD, MPH. "These survey data show, in stark terms, that practices will close because of this incident, and patients will lose access to their physicians. The one-two punch of compounding Medicare cuts and inability to process claims as a result of this attack is devastating to physician practices that are already struggling to keep their doors open."

AMA advocacy

Letter to CMS regarding MIPS recommendations

On April 11, the AMA sent a letter (PDF) to CMS urging the agency to implement a number of AMA recommendations on the Merit-based Incentive Payment System (MIPS) in the 2025 Medicare physician fee schedule proposed rule.

Letter to the National Association of Medicaid Directors

The AMA sent a letter (PDF) to the National Association of Medicaid Directors asking that it urge its members to take immediate action to assist physician practices in their states impacted by the Change Healthcare cybersecurity breach and resulting service outage, including taking advantage of flexibilities provided by CMS related to state plan amendments (SPAs) to provide advance payments to physicians under Medicaid.

Letter to the Administration urging regulatory flexibilities

The AMA sent a letter (PDF) urging the Department of Health and Human Services, the Department of Labor, and all health care system partners to use all regulatory flexibilities to continue supporting physicians and addressing the enormous interruption in physician practice operations caused by the Change Healthcare cybersecurity incident. The letter also asked the Departments to address a number of additional concerns that physicians have been voicing.

Advocacy encouraging CMS to extend MIPS hardship deadline

Based on AMA advocacy (PDF) and ongoing concern with the impact the Change Healthcare cybersecurity attack is having on physician practices, CMS has extended the 2023 MIPS data submission deadline until April 15. Notably, this attack on our nation's health care infrastructure coincides with the 2023 MIPS data submission window, which opened on January 2 and originally was scheduled to close on April 1.

The AMA welcomes this extension until April 15, but we are concerned the timeline is insufficient. Therefore, we will continue to push CMS to automatically apply the Extreme and Uncontrollable Circumstances (EUC) hardship exception to all MIPS eligible clinicians for the 2023 performance period. Alternatively, we will encourage CMS to reopen the hardship exception application for the 2023 performance period and allow eligible clinicians to claim an exception due to the Change Healthcare

cyberattack.

Letter to CMS urging financial relief

The AMA sent a letter (PDF) on March 8 urging CMS to provide financial relief from MIPS penalties for physicians and other clinicians impacted by the Change Healthcare cyberattack.

Letter to the National Association of Insurance Commissioners

The AMA sent a letter (PDF) on March 8 asking the National Association of Insurance Commissioners to urge its members to take immediate action to protect physician practices from the widespread impact of the Change Healthcare cybersecurity breach and resulting outage.

AMA statement expressing the need for advance funds for physicians

View the AMA's March 8 statement expressing the need for advance funds to physicians following UHG's announcement outlining the restoration timeline for the Change Healthcare claims system. The AMA also called for full transparency and security assurances from UHG.

Letter to HHS urging the department use all its available authorities

On March 4, the AMA urged U.S. Department of Health and Human Services (HHS) (PDF) Secretary Xavier Becerra to use all its available authorities to ensure that physician practices can continue to function, and patients can continue to receive the care that they need.

A press release was issued announcing the AMA letter sent to HHS Secretary Becerra.

Congressional activity

AMA statement for the record: May 1 Congressional hearing

The AMA submitted a statement for the record (PDF) in reference to a Senate Committee on Finance hearing entitled "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," which took place on May 1.

AMA comment letter: May 1 Congressional hearing

The AMA submitted a comment letter (PDF) in reference to a House Committee on Energy and Commerce Subcommittee on Oversight and Investigations hearing entitled "Examining the Change Healthcare Cyberattack," which took place on May 1.

AMA statement for the record: April 16 Congressional hearing

The AMA submitted a statement for the record (PDF) in reference to a House of Representatives Committee on Energy and Commerce Subcommittee on Health “Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack” hearing on April 16.

Bipartisan Congressional letter to HHS

On March 19, Representatives Mariannette Miller-Meeks (R-IA) and Robin Kelly (D-IL) along with 94 bipartisan members of the House of Representatives, sent a letter (PDF) to HHS Secretary Xavier Becerra alerting the administration of the ongoing challenges physicians and patients are continuing to experience as part of the Change Healthcare Cyberattack. In addition to highlighting the inability of physician practices to file claims and receive payment, the letter urged CMS to clarify why they issued such stringent repayment terms for advance payments on March 9. The letter also highlighted how many patients are being forced to pay out-of-pocket for many pharmaceuticals and health care services stemming from the cyberattack, as well as pressed the department for answers as to how it proposes to safeguard patients from the negative impact of their private health care being inappropriately disclosed to malicious actors.

Cybersecurity updates

In response to active exploitation of a cybersecurity vulnerability, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) have released a joint announcement on the cyber-attack that impacted Change Healthcare. The advisory details the attack and provides information for medical practices and information technology staff to help strengthen your organization’s cybersecurity.

HHS/CMS resources for practices

HHS/OCR FAQs concerning HIPAA

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) posted a new webpage to share answers to frequently asked questions (FAQs) concerning HIPAA and the

cybersecurity incident impacting Change Healthcare, a unit of UnitedHealth Group (UHG), and many other health care entities. The cyberattack is disrupting health care and billing information operations nationwide and poses a direct threat to critically needed patient care and essential operations of the health care industry.

Apply by April 15 for a MIPS hardship exemption

Based on direct AMA advocacy to the Administration, CMS has now reopened the 2023 MIPS Extreme and Uncontrollable Circumstances (EUC) hardship application due to the Change Healthcare cyberattack. The deadline to apply for an exemption is **April 15, 2024**. We are flagging this now due to the short timeline to take advantage of the flexibility. The 2023 MIPS EUC hardship exemption is not automatic and requires physicians to apply. If a physician or practice has already submitted data and would like to take advantage of this flexibility, it requires logging into the CMS portal and updating the submission.

If a physician or practice would like to still be scored on the 2023 MIPS Program, the extended deadline to submit data remains **April 15, 2024**.

HHS compilation of health insurer resources

On March 25, the Department of Health and Human Services (HHS) distributed these resources (PDF) to assist physicians, pharmacists and hospitals, with the aftermath of the Change Healthcare cybersecurity attacks. The AMA told HHS on a number of occasions that physicians were having difficulty securing information from health insurers about the availability of assistance with payments, flexibilities from administrative requirements, and additional contact information for troubleshooting due to the Change Healthcare cybersecurity attacks. Other interested parties raised similar issues. HHS responded by assembling these resources from health insurers. Please note that the HHS cover letter points out that the resource document contains a national contact person for each plan, though HHS urges physicians, pharmacists and hospitals to reach out first to their health insurer's regional contact. If these contacts do not respond to inquiries, please contact HHScyber@hhs.gov.

CMS FAQs

On March 13, CMS published FAQs related to the Change Healthcare/Optum payment disruption accelerated and advance payments. These go into detail about what services qualify for accelerated and advance payments, application criteria, terms of repayment, financial concerns and other topics.

CMS' Medicare advance payments program

The Centers for Medicare and Medicaid Services (CMS) on March 9 announced a new opportunity for physicians impacted by the cyberattack and resulting disruptions with Change Healthcare to request advance Medicare payments to help with cash flow disruptions. The details of the program, terms and the steps needed to apply can be found in the links below.

- Fact sheet
- CMS statement

CMS takes steps to assist physicians

CMS is taking steps to assist physicians in the wake of the Change Healthcare cybersecurity attack.

The AMA credits the Department of Health and Human Services and CMS for responding to the urgent situation caused by the Change Healthcare cyber security incident and the unprecedent disruptions to medical practices and access to care. The newly announced flexibilities that have been put in place are a welcome first step, but the AMA is urging CMS to recognize that physicians are experiencing financial struggles that threaten the viability of many medical practices. Many physician practices operate on thin margins, and the AMA is especially concerned about the impact on small and/or rural practices, as well as those that care for the underserved. The AMA is urging federal officials to go above and beyond what has been put in place and include financial assistance such as advance payments for physicians.

HHS suggestions for protecting your networks

Cybersecurity experts and the HHS Administration for Strategic Preparedness and Response (ASPR) suggest taking these steps to protect your networks:

- With consideration of the written attestation from UHG that the Optum network is safe, organizations should evaluate their risk of using Optum, UnitedHealthcare and UHG systems.
- While UHG asserts that any system that is currently live and available is safe to use, organizations should evaluate their risks and make determinations if connections to Change Healthcare are appropriate at this time.

As part of your risk evaluation, health care organizations should consider the impacts of severing connectivity to Optum, which includes but is not limited to loss of prior procedure authorizations, electronic prescribing and other patient care functions. Ultimately, your organization should make its own determination on whether or not to block Optum specifically while considering all the risks and consequences of doing so.

Additional recommendations from AMA

Actionable next steps for impacted medical practices include (but are not limited to) the following:

- Communicate with your payors regarding payment workarounds to bypass disrupted Change Healthcare applications.
- Monitor the Change Healthcare Incident update website for relevant updates.
- Develop a set of security- and Incident-related questions or criteria for Change Healthcare to reestablish connectivity with Change Healthcare systems (e.g., what assurances can be provided that the risk has been contained and remediated? What security improvements have been implemented to help ensure similar incidents do not occur again? What personal information about our patients and/or clinicians has been compromised? What actions is Change Healthcare taking to protect those patients and/or clinicians?).
- Review HIPAA compliance programs, including (among others) written policies and procedures and security risk analyses.

Updates/resources from Change Healthcare and UHG

Change Healthcare's updates are posted on their website.

United Health Group (UHG) also created a website to provide updates on the cyber-attack.

UHG has put programs in place to assist physicians and other providers. The Temporary Funding Assistance for Providers is designed to help bridge the gap in short-term cash flow needs for physicians and other providers impacted by the disruption of Change Healthcare's services. In particular, UHG encourages practices that find the amount prepopulated in the Optum Pay system insufficient to meet their financial needs to please contact UHG—either submit a request through the Temporary Funding Assistance Program Form or call 1-877-702-3253.

All of these websites and the information they contain are provided by Change Healthcare/UHG and not by the AMA. The AMA has not reviewed the information for accuracy or content.

Additional resources

AMA has curated resources and has tips for physicians and health care staff to protect patient health records and other data from cyberattacks.