DHCS
CALIFORNIA DEPARTMENT OF HEALTH CARE SERVICES
Michelle Baass | Director

DATE: March 13, 2024

FROM: SARAH BROOKS
CHIEF DEPUTY DIRECTOR, HEALTH CARE PROGRAMS

TO: ALL MEDI-CAL MANAGED CARE PLANS

SUBJECT: FLEXIBILITIES TO ENSURE DELIVERY SYSTEM STABILITY FOLLOWING CYBERATTACK ON CHANGE HEALTHCARE

SUMMARY:

In light of the recent cyberattack on Change Healthcare, DHCS reminds Medi-Cal managed care plans (MCPs) of their legal and contractual obligation to timely pay claims submitted by Providers for Covered Services to Members. DHCS also strongly encourages MCPs adopt a set of flexibilities to ensure timely payment of claims and timely responses to authorization requests.

BACKGROUND:

Change Healthcare, a claims processing unit of UnitedHealth Group, was impacted by a cybersecurity incident on February 21, 2024.

Change Healthcare handles approximately fifty percent of all medical claims in the Unites States. Accordingly, the attack and subsequent disruption to Change Healthcare's operations is impacting the ability of tens of thousands of physicians, dentists, pharmacies, hospitals, and other Providers to submit claims and be reimbursed for the services they provide. Consumers, Providers, and pharmacies also report delays in being able to fill prescriptions and confirm insurance status.

DHCS also understands that the attack has impacted billing and care-authorization portals across the country. And, ultimately, if Providers are unable to submit claims and receive timely reimbursement, Providers may not be able to pay their employees or purchase necessary supplies and medications.

AUTHORITIES:

Legal and Contractual Requirements Regarding Timely Payment of Claims

MCPs must pay all claims within contractually mandated statutory timeframes[1, 2, 3] and in accordance with the timely payment standards in the Contract[4] for clean claims.[5]

The Contract requires that MCPs comply with HSC sections 1371 through 1371.36 and their implementing regulations, which govern Provider compensation.[6] In addition, the Contract requires adherence to federal Medicaid requirements which dictate 90 percent of all clean claims from practitioners, who are in individual or group practices or who practice in shared health facilities, be paid within 30 days of the date of receipt, and 99 percent of all clean claims be paid within 90 days of receipt.[7] If the MCP contests a portion of a claim, it must reimburse any uncontested portions of the claim within the statutory timeframes.[8]

The obligation of MCPs to comply with timely claims requirements is not deemed to be waived when MCPs require their medical groups, independent practice associations, or other contracting entities to pay claims for covered services.[9] An MCP's contract with a claims processing organization or a capitated Provider shall not relieve the MCP of its obligations to comply with timely claims requirements.[10]

The MCP Contract requires MCPs to maintain a management information system that contains Provider claims status and payment data.[11]

---

[1] MCP Contract, Exhibit A, Attachment III, 3.3.5, Claims Processing. MCP boilerplate Contracts are available at: https://www.dhcs.ca.gov/provgovpart/Pages/MMCDBoilerplateContracts.aspx. MCPs are also advised to review their specific MCP Contracts and amendments executed thereto.
[2] Health and Safety Code (HSC) sections 1371(a) and 1371.35(a). California law is available at: https://leginfo.legislature.ca.gov/faces/home.xhtml.
[3] Title 28, California Code of Regulations (CCR) section 1300.71(g). The CCR is searchable at: https://govt.westlaw.com/calregs/Search/Index.
[4] MCP Contract, Exhibit A, Attachment III, 3.3.5, Claims Processing.
[5] A "clean claim" is defined in Title 42, Code of Federal Regulations (CFR) section 447.45(b). The CFR is searchable at https://www.ecfr.gov/current/title-42.
[6] MCP Contract, Exhibit A, Attachment III, 3.3.5, Claims Processing.
[7] Id.; Title 42 CFR section 447.45.
[8] HSC sections 1371(a)(1) and 1371.35(a); Title 28 CCR section 1300.71(g) and (h).
[9] HSC sections 1371(c) and 1371.35(f).
[10] Title 28 CCR section 1300.71(e)(8).
[11] MCP Contract, Exhibit A, Attachment III, 2.1, Management Information System.

For more information regarding timely payment of claims, please refer to All Plan Letter (APL) 23-020.

PURPOSE OF LETTER:

Steps to Ensure Timely Authorizations and Claims Payments Following the Cyberattack on Change Healthcare

Given the magnitude of the cyberattack and the resulting disruptions, DHCS strongly encourages MCPs to take the following steps, if they have not done so already:

1. **Accept paper claims**: The Change Healthcare cyberattack has impacted Providers' ability to submit claims electronically. While some MCPs and Providers have established workarounds (e.g., using alternative clearinghouses), due to incompatibility and other issues, some Providers are unable to use an alternative clearinghouse. To prevent further payment delays, MCPs should waive any requirements to submit claims electronically, and should automatically accept paper claims from Providers, until Change Healthcare resumes operations or the MCP and Provider develop a suitable electronic workaround.
2. **Remove or relax timely claim filing requirements**: Given the difficulty or, in some cases, impossibility of submitting claims during this time, some Providers may not be able to submit claims within the normally required claims filing timelines. Accordingly, MCPs should temporarily remove or relax timely filing deadlines for impacted Providers. MCPs should not deny such claims as untimely and then require Providers to appeal under the "good cause" exception contained in the Knox-Keene Act (28 C.C.R. §1300.71(b)(4)), because doing so could further delay claims processing and reimbursement to Providers.
3. **MCPs' timely payment responsibilities:** MCPs that are unable to process payments due to the cyberattack should establish workarounds to ensure the MCP, and its Subcontractors, Downstream Subcontractors, and Network Providers, continue to pay claims within the statutory timeframes of 30 or 45 working days from receipt of a claim (28 C.C.R. §1300.71(g)).

   Additionally, if an MCP believes its claims systems are *not* impacted by the cyberattack, the MCP should nonetheless investigate whether the claims systems of its Subcontractors, Downstream Subcontracts, and Network Providers are impacted and whether that impact is disrupting timely claims submissions by and payments to Providers who deliver care to their Members. It is imperative that MCPs thoroughly investigate the impact on their ability to process and issue payments to ensure continued cash flow to Providers.

4. **Remove or relax prior authorization and other utilization management requirements**: The cyberattack and resulting outage impacts the ability of some Providers to submit prior authorization requests, which can delay care to enrollees. If the cyberattack has impacted an MCP's prior authorization processes, the MCP should consider either temporarily relaxing or removing prior authorization requirements or should develop an efficient workaround for Providers to ensure enrollees do not experience delays in receiving needed care.

5. **Publish, and update as needed, information for Providers on the MCP's website:** If MCPs have not already done so, they should post information on their websites and Provider portals to ensure Providers have up-to-date information about the extent to which the MCP's systems are impacted by the Change Healthcare cyberattack. That information should include MCP contact information for Providers experiencing difficulties submitting claims or getting prior authorizations. If an MCP's operations have not been disrupted by the cyberattack, the MCP should note that on its website.

6. **Work with Subcontractors, Downstream Subcontractors, and Network Providers on all of the above**: MCPs are responsible for ensuring that their Subcontractors and Network Providers comply with all applicable state and federal laws and regulations, Contract requirements, and other DHCS guidance, including APLs and Policy Letters.[12] These requirements must be communicated by each MCP to all Subcontractors and Network Providers.

   Some or all of an MCP's Subcontractors, Downstream Subcontractors, and Network Providers may rely on the same systems as the MCP to receive claims and administer payments. Accordingly, to the extent necessary, any flexibilities and/or workarounds an MCP develops to deal with the impact of the cyberattack should also apply to the services the MCP has delegated to its Subcontractors, Downstream Subcontractors, and Network Providers.

If you have any questions, please contact your Managed Care Operations Division (MCOD) Contract Manager.

[12] For more information on Subcontractors and Network Providers, including the definition and applicable requirements, see APL 19-001, and any subsequent APLs on this topic.