From: Chechi, Munir@DMHC

Subject: APL 24-005 - Change Healthcare Cyberattack

Date: Monday, March 11, 2024 11:26 AM

Attachments: APL 24-005 – Change Healthcare Cyberattack (3.11.24)

Dear Health Plan Representative,

The Department of Managed Health Care (DMHC) hereby issues this All Plan Letter (APL) 24-005 to encourage health plans to be flexible to ensure stability of the health care system following the cyberattack of Change Healthcare.

Thank you.

DEPARTMENT OF Managed Health Care

Gavin Newsom, Governor
State of California
Health and Human Services Agency
DEPARTMENT OF MANAGED HEALTH CARE
980 9th Street, Suite 500
Sacramento, CA 95814
Phone: 916-324-8176 | Fax: 916-255-5241
www.HealthHelp.ca.gov

ALL PLAN LETTER

DATE: March 11, 2024

TO: All Health Care Service Plans

FROM: Sarah Ream
Chief Counsel

SUBJECT: APL 24-005: Flexibilities to ensure delivery system stability following cyberattack of Change Healthcare

---

On February 21, 2024, Change Healthcare experienced a cyberattack that has significantly impacted Change Healthcare's ability to operate. Change Healthcare is a claims clearinghouse owned by United Healthcare Services, Inc.

Change Healthcare handles approximately fifty percent of all medical claims in the United 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.

The DMHC 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.

Given the magnitude of the cyberattack and the resulting disruptions, the DMHC strongly encourages health plans 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 plans 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, plans should waive any requirements to submit claims electronically, and should automatically accept paper claims from providers, until Change Healthcare resumes operations or the plan 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, plans should temporarily remove or relax timely filing deadlines for impacted providers. Plans 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. **Plans' timely payment responsibilities:** Plans that are unable to process payments due to the cyberattack should establish workarounds to ensure the plan or its delegates 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 a plan believes its claims systems are *not* impacted by the cyberattack, the plan should nonetheless investigate whether the claims systems of its delegates or vendors are impacted and whether that impact is disrupting timely claims submissions by and payments to providers who deliver care to the plan's enrollees. It is imperative that plans 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 a health plan's prior authorization processes, the plan 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 plan's website:** If plans 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 plans' systems are impacted by the Change Healthcare cyberattack. That information should include plan contact information for providers experiencing difficulties submitting claims or getting prior authorizations. If a plan's operations have not been disrupted by the cyberattack, the plan should note that on its website.

6. **Work with delegated entities on all of the above**: Some or all of a plan's delegated entities may rely on the same systems as the plan to receive claims and administer payments. Accordingly, to the extent necessary, any flexibilities and/or workarounds a plan develops to deal with the impact of the

cyberattack should also apply to the services the plan has delegated to other entities.

If you have questions regarding this APL, please contact your health plan's assigned reviewer in the DMHC's Office of Plan Licensing.