Information on the Change Healthcare Cyber-attack from the Urgent Care Association.

Hi All,

First, I hope that those who are impacted significantly are finding some time to take care of themselves personally right now. This is an incredible cognitive load that can impact mental health, especially for operators who were already struggling with margins and the market conditions. Our community has faced so much in the last 4 years and we are worn thin.

Sharing a video I recently released here with 5 tactics you can take starting immediately to help you stay afloat while you are impacted.

In addition, here are a few more things I am seeing that may be helpful for you to be aware of as you evaluate your operational response.

* You probably know you should not wait any longer to transition from Change Healthcare as a clearinghouse, but because of massive consolidation in the clearinghouse space over the past decade, all clearinghouses are affected in some way. It will depend on the payers you are submitting to the severity of impact. (Read a breakdown of the crisis and clearinghouse consolidation here from Out Of Pocket Healthcare. Bonus: it's satirical.)
* Some clearinghouses, such as Waystar, have established direct unidirectional connections with affected payers. Flag: *They can confirm transmission for timely filing, but cannot confirm receipt.*
* Providers have reported that they have received EFT’s,*but not the corresponding ERA to post or invoice the patient responsibility.*
* Some clearinghouses are recommending dropping to paper for claim submission (again for timely filing). Many providers had already begun this process. Flag: Providers across the nation will be dropping a surge of paper claims, and it could take months to unwind.
* As Molly mentioned, after the ransom was paid it increases the likelihood that cyberterrorists target other clearinghouses since they are all built on similar antiquated technology with a ton of tech debt. This is why it is vital that we backup and secure claims data, preferably with partners who are SOC-2 compliant.
* If you don’t watch the video I linked, I want to emphasize that collecting estimated patient responsibility, in full, at the point of service for commercial and self pay patients is going to be critical during this time to stay afloat. No one is going to be able to afford to bill patients later because ERA's/835's will be so delayed. If you can’t verify a patient’s insurance, you need to collect something. Establish a policy, communicate with the patient appropriately about the situation, and have a swift mechanism in place to refund later if you over-collected.

I genuinely hope this helps leaders in our community. My virtual door is open if anyone needs help.

Have a blessed weekend,

April Gillam

[**Don Self**](https://www.facebook.com/groups/1503414633296362/user/1189227882/?__cft__%5b0%5d=AZWiIaWiKeypET8joEzIKdi0oIUiVPHrEu7DDIr5Tr7hLcr8pdWqlOn54X4ixjPrww3U5oN-LPKdSTkU2s0eihSm7mepRqGd7Av9QHMHg-Xxn1QV5Ig58q007e6P3qcg0hLy7xD1Dgwzzp2LY9DHvi9F78seg1qQQ1Q0nJwVkHhOwpB8AtF594sY0wRK4TGWxCY&__tn__=R%5d-R)

Part of the problem is that the ransom was paid to one entity…. the one who did not actually have the 8 tb of stolen data, who then did not pay the agreed upon percentage ot the player who did the deed and has the data - so whether the data is ever released or not is another story - but as someone pointed out - now that they proved that it works - more companies will be hit. On another front, if you are trying to maximize your RHC income right now - immediately look to CCM and RPM as both not only increases the income of an RHC substantially - but both also help keep the patients out of the hospital and ER - which helps you towards your metrics. In the past month, I've had about a dozen RHCs and FQHCs reach out to me on these two services that Medicare allows you to job out or do pass-through billing on (so that you do not have to incur the cost of additional staff).

[**Mark Lynn**](https://www.facebook.com/groups/1503414633296362/user/534825756/?__cft__%5b0%5d=AZXjtQYlV9nl0KXdGsZ0zka7z_wBymwmHiZGHeKdA5twbfup8RhOiW8j-4697JT0SojrlJhrjeVCkdgNoca-FHSwIbtv06te5Nzft1yocZXhC-b46HU3AI5ZFudpmBWHSrAW4qebSuKUOgS-Kmk0H6C1tDpAmXN5AlpiB2R-eDXuqaSX5El_aw64jdJ94izKkWc&__tn__=R%5d-R)

Author

Admin

The title is wrong on the link above. It relates to the Change Healthcare cyber attack. Change Healthcare Security Incident

Update 03.11.24:

Complete the CHOPD Accelerated-Advance Payment Request Template.

Include the signature of the authorized official that is legally able to make financial commitments and assume financial obligations on behalf of the provider (digital – signature and a facsimile (fax) request is acceptable).

Providers/suppliers that are part of a health system may attach a list of Medicare IDs (PTANs)/NPIs to the form. The authorized representative must have authority to sign on behalf of all providers/suppliers included in the list.

Submit the completed and signed form to one of the following:

Email: CGS.ERS.CORR@cgsadmin.com

Fax: 1.615.664.5949

Mail:

CGS Administrators, LLC

ATTN: CFO Accelerated Payments

PO Box 20018

Nashville, TN 37202

To receive updates, please visit the Recent News section on our home pages and/or Join the Electronic Mailing List.