CLAY J. COUNTRYMAN
Partner
Clay.Countryman@bswllp.com

DIRECT DIAL: (225) 381-8037
CORPORATE PHONE: (225) 387-4000
FAX: (225) 381-8029
One American Place, 23rd Floor
301 Main Street
Baton Rouge, LA 70821-3197
www.bswllp.com

March 6, 2024

Mr. Richard L. Gundling
Healthcare Financial Management Association
Senior Vice President Professional Practice
1015 15th Street NW, Suite 600
Washington, DC 20005

Dear Rick:

RE: **Change Healthcare Cyberattack – Recommendations for HFMA Members Updated Through March 4, 2024**

This letter is to provide some recommendations and resources for Healthcare Financial Management Association (HFMA) members to consider in managing the operational and financial impact from the cyberattack on Change Healthcare that occurred.[1] Change Healthcare, which is the claims processing platform for Optum and is part of UnitedHealth Group, experienced a cyberattack on Wednesday February 21, 2024.

This cyberattack on Change Healthcare continues to have a tremendous impact on healthcare providers ability to verify patients' health insurance coverage, process claims and receive payment from many payers, exchange clinical records with other providers, provide cost estimates and bill patients, among many other operational and financial impacts. The lack of access to Change Healthcare's platform is causing significant cash flow issues for many provider organizations and impacting the delivery of health care services.

Recommendations and potential resolutions for healthcare organizations related to the Change Healthcare cyberattack are evolving daily at this point. Healthcare organizations should be aware of potential organizational and financial impacts and the evolving ways that these impacts can be mitigated by their organizations.

[1] Chris Vidrine, who is an associate in the BSW healthcare group, contributed to this summary and identification of recommendations for HFMA members regarding the cyberattack on Change Healthcare.

The following is a summary of some of the significant issues and recommendations for healthcare organizations to date for HFMA members to consider:

1. Connection to the Change Healthcare Systems

An on-going decision for healthcare organizations is whether to re-connect or to maintain disconnection from Optum, UnitedHealthcare and UnitedHealth Group systems that UnitedHealthcare had announced were not affected by this cyberattack. Change Healthcare has announced that it has taken appropriate action to contain the incident so that customers and partners do not need to sever network connections to available vital services.

Common healthcare industry recommendations include the following:

- Non-Impacted Change Healthcare Systems. Each health care organization should continue to monitor and independently evaluate information provided by Change Healthcare to make its own risk-based decisions regarding nonimpacted systems identified by Change Healthcare. When considering connectivity to nonimpacted systems, each health care organization should weigh possible clinical disruptions and business impacts caused by severing the connection to nonimpacted Optum, Change Healthcare, UnitedHealthcare and/or UnitedHealth Group systems.

- Impacted Change Healthcare Systems. A common recommendation is that all health care organizations maintain disconnection from applications specified by Change Healthcare that **remain unavailable due to this cyberattack** as identified by Change Healthcare as unavailable on the following webpage: https://status.changehealthcare.com/.

2. Addressing Operational Impacts – Recommendations to Address the Source of Change Healthcare Cyberattack

- Change Healthcare acknowledged during the week of February 26th that the attack was by ALPHV Blackcat. The Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, and Department of Health and Human Services issued an updated joint advisory #StopRansomware: ALPHV Blackcat. The updated advisory provides new indicators of compromise and tactics, techniques and procedures associated with the ALPHV Blackcat ransomware as a service.

3. Addressing Operational Impacts – Patient Care

- Healthcare providers should consider the Sentinel Event Alert issued by The Joint Commission that addresses risks associated with cyberattacks and provides recommendations on how healthcare organizations can prepare to deliver safe patient care in the event of a cyberattack. A copy of The Joint Commission alert is available at:

https://www.jointcommission.org/resources/sentinel-event/sentinel-event-alert-newsletters/sentinel-event-alert-67-preserving-patient-safety-after-a-cyberattack/

4. Mitigation Actions to Address February 21, 2024 Change Healthcare Cyberattack

The following are recommended mitigation practices for cyberattacks that healthcare organizations should consider on an ongoing basis, including in response to the Change Healthcare cyberattack:

- Healthcare organizations running any affected application by the Change Healthcare cyberattack should immediately update the affected software, and update devices as soon as possible.

- Healthcare organizations should review cyber and business interruption insurance policies for potential areas of coverage and required actions to mitigate further damages. Many policies require prompt notification after discovery of a potential security incident or business interruption, so organizations should act quickly to determine whether insurance coverage could be implicated by this incident.

- Healthcare organizations should consider the following actions to mitigate against the threat of ransomware:

  - Network defenders should enter their indictors of compromise into their network defenses and threat hunting tools as soon as possible.
  - Routinely take inventory of assets and data to identify authorized and unauthorized devices and software.
  - Prioritize remediation of known exploited vulnerabilities.
  - Enable and enforce multifactor authentication with strong passwords.
  - Close unused ports and remove applications not deemed necessary for day-to-day operations.

- Organizations should also use this opportunity to test the security, redundancy and resiliency of their network and data backups to ensure they remain offline.

- Backup technology is generally recommended which renders the backups "immutable" — unable to be deleted, altered or encrypted.

- Ensure that all high criticality, known and exploited vulnerabilities have been patched, especially any which are internet facing.

- Review and test cyber incident response plans, and ensure they are well coordinated and integrated with emergency management plans.

- Review business and clinical continuity downtime procedures to ensure mission critical and life critical functions could sustain a loss of information, operational and medical technology for up to 30 days.

5. Addressing Financial Impacts

One of the most significant impacts of the shutdown of Change's platform is that healthcare organizations are no longer able to send claims information through Changes clearinghouse platform and are no longer able to receive claim information back from payers through the platform.

UnitedHealthcare Group announced on March 1, 2024 that it created a Temporary Funding Assistance Program for healthcare organizations impacted by the cyberattack on February 21, 2024. There have also been several requests to Congress to provide financial assistance to affected healthcare organizations (such as accelerated payments from the Medicare program).

Change Healthcare announced on Friday, March 4, 2024, a Temporary Funding Assistance Program for healthcare organizations. However, many healthcare providers and provider associations have immediately articulated concerns with this "assistance program" because it only provides very limited relief for providers who cannot bill payers due to the ongoing disruption of Change Healthcare's clearinghouse and claims submission systems, and that the terms and conditions of the "assistance program" agreement are shockingly onerous.

Healthcare organizations should follow the requests to the Medicare program to provide for Medicare accelerated programs, similar to the Medicare accelerated payments provided during the COVID-19 pandemic.

6. Assessment of Impacts and Potential Breaches of Healthcare Provider's Information

Healthcare organizations should have their cybersecurity and/or IT teams perform an immediate investigation and review of the potentially affected system(s), identifying and isolating any anomalous behavior until remediation can occur. Additionally, healthcare organizations should immediately review their HIPAA compliance policies and procedures to prepare for potential consequences, including breach notifications, security audits, and civil litigation.

7. Management of Claims Processing and Claims Transactions Clearinghouses

Organizations should communicate with EMR and IT vendors about alternative claims submission processes that may be available. Additionally, organizations should communicate directly with payors to potentially create alternative methods of payment.

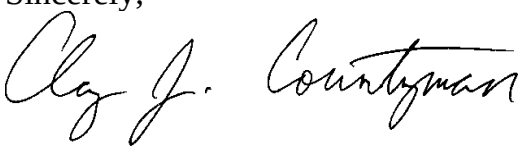
8. **Action Steps To Address Financial and Related Issues and Potential Recovery**

Some actionable next steps (which are evolving with new information) for health systems and other healthcare providers to consider include the following:

- Communicating with payors regarding payment workarounds to bypass disrupted Change Healthcare applications. Depending on your individual payer contracts, healthcare providers may also have the right to be paid interest on claims that were not paid timely.
- Monitoring the Change Healthcare incident update website.
- Monitoring updated advisories by the Healthcare Financial Management Association (HFMA) and American Hospital Association (AHA) for updates and recommendations, including recommendations regarding potential claims of processing- and payment-related cashflow interruptions
- Notifying cyber policy insurance carriers and other applicable insurers of any business interruptions and of a potential security incident, and be ready to immediately track any potential impacts from a security incident from the Change Healthcare cyberattack.
- Ongoing communication with payors regarding payment workarounds to bypass disrupted Change Healthcare applications.
- Developing a set of security- and Incident-related questions or criteria for Change Healthcare in order 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?).
- Reviewing CISA recommendations to reduce the likelihood and impact of ALPHV Blackcat ransomware and data extortion incidents.

In short, these are only some of the issues and recommended steps to address these issues to date from the Change Healthcare cyberattack. Health care organizations are strongly encouraged to monitor daily these issues and evolving new issues and ways to address them.

Sincerely,



Clay J. Countryman

CJC/ct