May 1, 2024

The Honorable Ron Wyden
Chairman
Senate Committee on Finance
215 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mike Crapo
Ranking Member
Senate Committee on Finance
215 Dirksen Senate Office Building
Washington, DC 20510

Re: MGMA Statement for the Record — Senate Committee on Finance Hearing, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next"

Dear Chairman Wyden and Ranking Member Crapo:

The Medical Group Management Association (MGMA) thanks you for holding this important hearing examining the Change Healthcare cyberattack and what comes next. MGMA members were significantly impacted by the cyberattack and continue to deal with the fallout. We appreciate the Committee reviewing how this caused so much disruption to our nation's health system and examining policies to help mitigate future cyberattacks.

With a membership of more than 60,000 medical practice administrators, executives, and leaders, MGMA represents more than 15,000 group medical practices ranging from small private medical practices to large national health systems, representing more than 350,000 physicians. MGMA's diverse membership uniquely situates us to offer the following policy recommendations.

On Feb. 21, Change Healthcare experienced a cyberattack that critically impacted the U.S. healthcare system, causing unprecedented outages. Change Healthcare touches one in three patient records and processes 15 billion healthcare transactions annually.[1] With one corporate entity providing so many services to such a wide swath of the nation's healthcare ecosystem, the disruptions caused by the malicious cyberattack resulted in substantial harm.

Impact of the Change Healthcare cyberattack on medical groups

Given the breadth of services Change Healthcare offers, MGMA members felt myriad negative consequences following the cyberattack, including: severe billing and cash flow disruptions, inability to submit claims, limited or no electronic remittance advice (ERA) from health plans, electronic prescriptions could not be transmitted, lack of connectivity to data infrastructure, health information technology disruptions, and much more. Physician practices diligently instituted workarounds for various processes to remain operational, which required significant labor costs and time to institute, diverting critical resources from patient care.

[1] Department of Health and Human Services, Letter to Health Care Leaders on Cyberattack on Change Healthcare, March 10, 2024.

The lack of cash flow that resulted from the Change Healthcare attack led to medical groups having to make difficult financial decisions as it was early in the year and practices already had limited working capital on hand due to tax considerations. Smaller practices were particularly affected given their tight margins and had to utilize lines of credit with high interest rates just to keep their doors open. Practices have had to make drastic payroll decisions in the wake of the attack; one MGMA member's statement to CNN sums up the gravity of the situation: "We are hemorrhaging money, this will probably be the last week we can keep everybody on full time without having to do something."[2]

While some of Change Healthcare's systems have come back online, effects of the attack still remain — there's an extensive backlog of claims being processed, some groups are still not receiving ERAs impacting their ability to reconcile claims, and practices are still utilizing resource-intensive workarounds. Further, we still do not know the full extent of the cyberattack as both Change Healthcare and law enforcement authorities are investigating the data breach. In totality, the Change Healthcare cyberattack continues to ripple throughout this nation's health system.

Federal response and policy considerations to support physician practices

As the scope of the cyberattack became apparent, MGMA wrote to the Department of Health and Human Services (HHS) on Feb. 28 expressing the severity of its impact to medical groups and advocating for the agency to use all tools at its disposal to mitigate the damage.[3] Thankfully, HHS instituted numerous flexibilities in response and offered accelerated and advanced payments to hospitals and providers to help mitigate the consequences from the cyberattack. We appreciate the Department heeding our call and swiftly acting to assist practices.

The cyberattack on Change Healthcare made it evident that there are significant vulnerabilities in our healthcare system, which must be addressed — especially as the threat of such attacks only continues to rise. **Moving forward, health plans, clearinghouses, and other third-party vendors must have safeguards and contingency plans in place to better protect physician practices from such significant cash flow and administrative impacts resulting from a cyber incident.**

The Committee should examine whether further authorities and flexibilities should be granted to federal agencies responding to future attacks to support physician practices. Specifically, the Committee should ensure that the statute governing advanced payments to Part B providers allows for a quick response time from HHS to a future attack, and that repayment terms are not onerous, adding another stressor during a time of acute uncertainty. Additionally, the Committee should review whether other policies should be introduced such as waiving timely filing requirements for health plans, reducing prior authorization burden, and relaxing other requirements as it may be impossible to fulfill them with such widespread outages. This would be a significant step to allow practices to function with a semblance of efficiency during a cyberattack of this size.

Physician practices must continue to work to ensure they have adopted ironclad cybersecurity policies and procedures to best protect the data of their patients and their ability to provide high-quality care. When contemplating the fallout, we urge against establishing penalties, or conditioning relief funds, for medical

---

[2] Sean Lyngaas, CNN, "*'We're hemorrhaging money': US health clinics try to stay open after unprecedented attack,"* March 9, 2024.
[3] MGMA, Letter to CMS on Change Healthcare Cybersecurity Attack, Feb. 28, 2024.

groups in response to cyberattacks perpetuated against other healthcare actors. There are a multitude of security and data privacy regulations governing medical groups; introducing barriers to future relief would work against supporting medical groups' ability to operate in the face of considerable interruption.

It is important to note that physician practices have access to widely different levels of cybersecurity resources depending on their size. The President's budget acknowledged the need to bolster cybersecurity resources within the healthcare sector, allocating $800 million to assist "high-need, low-resourced" hospitals to help implement cybersecurity practices.[4] The budget also proposed $500 million for an incentive program for advanced cybersecurity practices for hospitals. **Ensuring that all physician practices are afforded resources similar to those proposed for hospitals is critical**. We support practices incorporating voluntary cybersecurity goals, like those recently published by HHS, to bolster their defenses against future attacks.

These are sophisticated criminal cyberattacks often sponsored by nation states that are not only impacting healthcare but many other industries in addition to federal, state, and local governments. **Exacerbating a terrible situation by adding further penalties to medical groups beyond what is already in place would be overly punitive for practices not responsible for the attack and operating in full compliance.** Resources should be devoted to law enforcement agencies to bolster their actions to combat these cyberattacks and prevent them before they begin. Our nation's law enforcement agencies have the expertise and training to stop these criminals — we should ensure they have every resource necessary at their disposal.

Breach of protected health information

Change Healthcare is currently undergoing an investigation into the data breached during the cyberattack, but "based on initial targeted data sampling to date, the company has found files containing protecting health information ("PHI") or personally identifiable information ("PII"), which could cover a substantial proportion of people in America."[5] MGMA appreciates recent public statements from UnitedHealth Group committing to "provide appropriate notifications" and stating that it "has offered to make notifications and undertake related administrative requirements on behalf of any provider or customer."[6] At the same time, no prudent medical group can rely on vague promises in a press release containing no specifics with respect to either timing or implementation.

Medical groups currently face mounting concerns about their own regulatory exposure should United not fulfill these promises to the satisfaction of the Department of Health and Human Services Office for Civil Rights (OCR). Further, as more patients become aware of the possible disclosures of their sensitive PHI and PII, they will turn to their providers for information and assurances, neither of which can currently be provided.

MGMA wrote to OCR last week asking for clarity from their office that:

1. responsibility for breach notifications rests solely with Change and UnitedHealth Group;
2. providers that are completely innocent in this unique situation will be spared any regulatory scrutiny; and

[4] Department of Health and Human Services, Fiscal Year 2025 Budget in Brief, pg. 80, March 11, 2024.
[5] UnitedHealth Group Press Release, April 22, 2024.
[6] *Id.*

3. OCR will ensure that Change and United fulfill the promises they have made in a prompt and transparent manner.[7]

We recommend the Committee works to ensure that UnitedHealth Group fulfils their promises, and that OCR provides a clear statement that the responsibility for the HIPAA-required breach notifications falls solely with UnitedHealth Group and Change Healthcare.

Conclusion

MGMA looks forward to working with the Committee to reinforce the resiliency of the cybersecurity defenses for this nation's health system. It is critical to ensure physician practices can continue providing high-quality patient care in the face of substantial disruptions. If you have any questions, please contact James Haynes, Associate Director of Government Affairs, at jhaynes@mgma.org or 202-293-3450.

Sincerely,

/s/

Anders Gilberg
Senior Vice President, Government Affairs

[7] MGMA, letter to OCR on Change Healthcare and breach notifications, April 25, 2024.