Three Minute Read™

Insights from the Healing American Healthcare Coalition™

SPECIAL EDITION - CYBERSECURITY April 2024-4

HEALING AMERICAN HEALTHCARE COALITION

From the Editor: This **TMR** Special Edition focuses on the cybersecurity challenges raised by the Change Healthcare cyberattack. Click on the headline to read the full article. If you enjoy **TMR's** coverage of emerging issues, please upgrade to a paid subscription here.

Medical Providers Still Grappling With UnitedHealth Cyberattack: 'More Devastating Than Covid', by Samantha Liss, KFF Health News, 4/19/24

TMR Topline – Two months after the cyberattack on Change Healthcare, providers are still grappling with the fallout although UnitedHealth told shareholders on a 4/16 earnings call that business is largely back to normal. Edina MN therapist Emily Benson said *"This was way more devastating than Covid ever was"* for her eight-person practice. Instead of electronic remittances, mailed forms must be processed manually, a time-consuming process. Nearly 1/3 of US medical claims pass through the Change platform. The company has encouraged providers to reach out to it directly via its website, and has loaned providers $7 billion so far. The House Energy and Commerce Health Subcommittee held a hearing 4/16 seeking answers on the severity and damage the cyber-attack caused. Chair Brett Guthrie (R-Ky.) said a provider in his hometown is still grappling with fallout from the attack and losing staff because they can't make payroll. Rep. Frank Pallone Jr. (D-N.J.) voiced concern that a *"single point of failure"* reverberated around the country, disrupting patients' access and providers' financial stability. The Committee had sent UnitedHealth CEO Andrew Witty detailed questions ahead of the hearing, but the company did not send a representative.

UnitedHealth Group℠

Lawmakers rip United-Health at Change Healthcare hearing, by Michael McAuliff, Modern Healthcare, 4/16/24

TMR Topline – Lawmakers on the House Energy and Commerce Committee expressed dismay at United-Health's absence from its first hearing on the Change Healthcare breach and cybersecurity. Lawmakers and witnesses raised a number of issues related to United-Health Group, such as how much the company's size and vertical integration allowed and contributed to the impacts of the cyberattack, how well or poorly it is responding, whether it is doing enough to help providers, and what lessons it has learned that may apply more broadly. Witnesses agreed that big, vertically integrated healthcare companies are a national security vulnerability when they are insecure. UnitedHealth CEO Andrew Witty has agreed to appear for questioning at a future date.

hfma

Cyberattack on Change Healthcare brings turmoil to healthcare operations nationwide, by Nick Hut, HFMA, 4/23/24

TMR Topline – The Healthcare Financial Management Association has been monitoring the impact of the cyber-attack on its members and posting regular updates on its website. In the 4/23 update, UnitedHealth Group (UHG) confirmed that *"a substantial proportion of people in America"* are at risk due to the exposure of protected health information (PHI). UHG is offering to make the required notifications *"and undertake related administra-tive requirements on behalf of any provider or customer"* regarding the data breach. HIPAA-covered entities are required to make timely breach notifications to HHS and affected individuals stemming from such attacks.

According to the Wall Street Journal, hackers penetrated Change Healthcare's systems more than a week before launching the 2/21 ransomware strike. The vulnerability

apparently stemmed from inadequate remote-access authentication, including a lack of multifactor authentication. UHG reportedly paid a $22 million ransom to the Blackcat group in early March. After Blackcat allegedly cut its cyberattack partners out of the payment, RansomHub announced it had four terabytes of PHI and other files from the attack and sought another payment.

Hackers start selling Change Healthcare data, by Giles Bruce, Becker's Hospital Review, 4/17/24

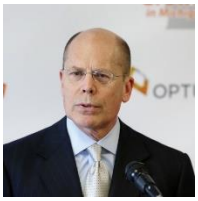
TMR Topline – The RansomHub cybercriminal gang reportedly has begun to sell patient data that were stolen in the Change Healthcare cyberattack. RansomHub says it obtained information from several major payers in the hack, and the payers can contact the gang — likely to negotiate ransom payments — if they want to prevent the data from being leaked or sold.

TMR's Take: Reporting on the cyberattack in its 3/6 issue, **TMR** commented: *"With 2023 revenues of $371.6 billion and earnings of $32.4 billion, the oligopolistic UnitedHealth Group is the largest healthcare company on the Fortune 500 list, ranked #5. Did the company place profits above providers, payers, pharmacies and patients, leaving its customers exposed to cyberattacks? Did it invest sufficient resources in system redundancy and cybersecurity, or did it prioritize hitting profit goals?"* UHG now has confirmed that its Change Healthcare subsidiary, processing about 15 billion transactions yearly, handling an estimated 1/3rd of US patient records, did not have multifactor authentication in place for remote access.

UnitedHealth CEO: '[It's] important for the country that we own Change Healthcare', by Andrew Cass, Becker's Hospital Review, 4/17/24

TMR Topline – On its 4/16 earnings call, UnitedHealth CEO Andrew Witty called Change an important acquisition for the company, adding *"I think [it's] important for the country that we own Change Healthcare. This attack would likely still have happened, and it would have left Change Healthcare, I think, extremely challenged to come back. Because it was a part of UnitedHealth Group, we've been able to bring it back. We're going to bring it back much stronger than it was before."* The DoJ had opposed the company's acquisition of Change, the largest claims clearinghouse in the US, arguing that the merger was anticompetitive because Change has access to data from insurer customers. The company argued that the deal should go through because there are policies in place to protect sensitive data.

At the August 2022 bench trial, Witty said companies under the Optum umbrella are kept *"strictly at arms' length,"* adding that the insurer and Change operate in a supplier-purchaser relationship rather than as two parts of an enterprise. The deal closed October 2022. The DoJ is continuing to scrutinize the company. Neither DoJ nor the company would comment publicly on the investigation.



UnitedHealth chair, execs sold $102M in stock before DOJ probe became public, by John Tozzi and Anders Melin, Bloomberg, 4/15/24

TMR Topline – UnitedHealth Group Chairman Stephen Hemsley and three senior executives netted a combined $101.5 million from stock sales made between 10/16/23, a week after receiving notice of the DoJ probe, and 2/24/24, the day before Bloomberg News and others published stories about the investigation. The stock dropped after the investigation was widely reported. When asked about the trades, a spokesperson said, *"these directors and officers followed our protocols and received approval from the company."* Hemsley has served as chairman since 2017 after serving as CEO for the prior decade. The DOJ is reviewing whether UnitedHealth's acquisitions have consolidated its position in some markets in a way that violates antitrust laws.

TMR's Take: Is this corporate chutzpah or just unbridled greed? Perhaps a lot of both. Instead of being embarrasssed by their failure to adequately protect customers' PHI, the UHG executives appear to be completely clueless. The May 1 Congressional hearings should see a lot of fireworks. It's time to replace UnitedHealth Group with universal healthcare, and explore moving the US closer to the systems that produce better outcomes at lower cost in France and Germany. The Allcare Plan detailed in "Healing American Healthcare: A Plan to Provide Quality Care for All, While Saving $1 Trillion a Year describes such a plan for the US. It's available in both soft-cover and eBook versions. Click Here to buy it.