COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 24, Number 5. May 09, 2024 'I Will Not Rest'; 'I Am All In': Remarkable Breach Hearing Sees Pledges by UHG CEO, Sen. Wyden

By Theresa Defino

United Healthcare Group (UHG) CEO Andrew Witty was in a board meeting on Feb. 21 when officials interrupted with the news that Change Healthcare—a clearinghouse UHG subsidiary Optum had purchased for $1.3 billion in October 2022—was in the throes of a ransomware attack.

Hackers had actually entered the system nine days earlier via a single, external "portal" that—contrary to UHG policy—was not protected with multi-factor authentication.

"The minute we knew about this, in fact, even before I'd been briefed, our team had followed the right steps and disconnected Change from all other connections because it was critical to prevent the infection [from] affecting any other provider or network in the country," Witty recently testified before the Senate Finance Committee.[1] "That worked. We know that did not happen. So, we contained the blast radius to just Change."

But however "contained" Witty believed the blast to be, months later, the ripples continue as UHG itself now works to identify—and notify—affected patients, who likely number in the millions. Witty described other steps UHG took after the biggest health care data breach in history, including building a new system "from scratch," details that may prove instructive to other covered entities (CEs) and business associates (BAs). For example, Witty said he alone decided to pay a ransom to get data back but did not mention the amount, reported to be $22 million.[2]

UHG—along with providers and other customers—is still struggling to return to what Witty termed "pre-incident" operations. For their part, members of Congress and the HHS Office for Civil Rights (OCR) are eager to learn why the server was left vulnerable, if UHG will face sanctions once OCR completes the investigation it announced in March and what new laws or regulations might be needed.

At the hearing, Sen. Ron Wyden, D-Ore., Finance chair, floated the idea of creating mandatory minimum cybersecurity standards for CEs and BAs and perhaps others, a concept Witty embraced (from the witness table, at least).

Wyden also argued that because of its size—UHG is the nation's largest insurer in terms of revenue—it is among those with "an obligation to protect their customers and to lead on this issue" and that the firm had "let the country down" by not preventing the attack and by employing inadequate recovery efforts.

Ensuring the security of health care data "is one of the most important issues I've taken on," Wyden said. "The intersection of health policy, economics, and national security is now front and center. And I am all in on this."

UHG Repels Attacks 'Every 70 Seconds'

Witty repeatedly apologized and expressed regret about the breach, including UHG's initial handling of it. And while he took responsibility, Witty said health care as a whole needs help "to reduce the attack velocity." According to his written testimony, given to the committee in advance and posted online, UHG "alone repels an

attempted intrusion every 70 seconds—thwarting more than 450,000 intrusions per year."[3]

Following the breach, firm officials "deployed the full resources" of UHG," Witty testified. "I want to assure the American public we will not rest—I will not rest--until we fix this," he said, adding that "cyber experts continue to investigate the incident."

The May 1 hearing was remarkable for a variety of reasons, including that details about how firms handle ransomware attacks aren't often discussed in public. Senators were rarely argumentative with Witty, and the hearing contained less grandstanding than usual for Capitol Hill. Senators seemed genuinely interested in what Witty had to say and shared with him details of providers in their states that are still reeling and need UHG's help. Witty promised to provide assistance.

Wyden: Breach Created 'Financial Bedlam'

As chair, Wyden controlled the hearing and gave an opening statement (as did Ranking Member Sen. Bill Cassidy, R-La). He used his time not only to admonish UHG but criticize OCR, calling its settlements following other breaches "a slap on the wrist" and noting that there has not been a "proactive cybersecurity audit in seven years." Wyden also suggested that, given its size, UHG should be examined by the government for antitrust issues.

Other Senators asked Witty—the only person to testify and who did so for 150 minutes without a break—what lessons UHG had learned so far, and extracted a promise that he will keep sharing what he uncovers.

The senators also wanted to know what the FBI and other governmental agencies did right and wrong and what they should do better next time.

Wyden and other senators were clearly frustrated by the breach and UHG's handling of it, and the continuing lack of basic details. Witty said he, too, was frustrated.

"United Health Group has not revealed how many patients' private medical records were stolen, how many providers went without reimbursement, and how many seniors were unable to pick up their prescriptions as a result of the hack," Wyden said.

He called it a "failure" that Witty, "months in, can't figure out how many people have had their data stolen." The attack and its aftermath, Wyden said, left health care providers nationwide "in a state of financial bedlam."

Some Change Systems Were 40 Years Old

Wyden bemoaned the fact that, despite its length, the hearing didn't reveal "what data was stolen. And I'm not convinced that we are gonna find that out anytime soon. We may never find it out," he said.

This attack was predictable and predicted—and there will be others, said Sen. Mark Warner, D-Va., long a champion of increased data privacy and security requirements that—to date—have not made it into law.

In questioning Witty, Warner was incredulous that UHG—"the biggest in the business"—had not corrected the lack of multi-factor authentication it knew existed in Change Healthcare "two years into the acquisition," in violation of UHG's companywide policy of multi-factor authentication on all external-facing systems.

"Why," asked Warner, "why was it taking so long" to implement the required controls?

Although Witty thanked Warner for the question, he couldn't answer it. "That is very much still...we're just trying to dig through [to learn] exactly why that server had not been protected by multi-factor authentication,"

Witty said. "I'm as frustrated as anybody about that fact. We are working to try and understand exactly why it was not covered at the time."

Experts have long warned that organizations engaging in mergers and acquisitions must conduct due diligence to learn whether what their acquiring has appropriate security and privacy processes in place, and ensure gaps are remediated. Although not required by the Security Rule, multi-factor authentication is considered "Security 101," in the words of some senators, and is ubiquitous in everyday transactions.

In response to a related question from Sen. John Barrasso, R-Wyo., Witty said UHG had been "upgrading [Change's] technology since we acquired it" and acknowledged that Change was founded in 2007. But Witty said some, "of the legacy systems in that company go back 40 years."

Sen. Maggie Hassan, D-N.H., pointed out that the HIPAA breach notification clock was ticking and that UHG would miss the 60-day deadline. "To meet your HIPAA obligations, you need to at least send preliminary notifications to individuals so that they can take protective actions like monitoring their bank accounts, changing passwords, and enrolling in the credit monitoring system that UnitedHealthcare has set up," Hassan said. She asked when notification would occur.

"In regard to your question, this is our top priority, to go as fast as we can to understand this. Of course, what we're trying to [do is] make sure that the information and the people we communicate with is right," Witty said. "First and foremost, we're working with regulators to understand how best to do that. We were held up in the process because it took time to get the original data set back. We only got hold of that in mid-March. We are working on that and we're working with regulators on how to do exactly as you described."

Exclusivity Clauses Thwarted Options

Hassan responded that UHG should "immediately" notify affected individuals and "use United Health's substantial resources to do more for patients who were exposed in this hack, including by offering comprehensive identity protections to individuals beyond the two years of credit monitoring that you're offering right now."

Wyden scoffed at UHG's provision of breach services, calling credit monitoring "the thoughts and prayers of data breaches. This is absolutely inefficient."

Hassan also noted that the impact of the breach was compounded by UHG's near-exclusive control of the clearinghouse market and its requirement, in some instances, of exclusivity. Such arrangements are bad for security because providers can't have redundant or backup billers. Providers "have told me that they're no longer comfortable with the risk of relying on a single system for processing their payments," Hassan said.

UHG is abandoning its insistence on exclusivity "because we agree with you that having business redundancy is an important backup to technological risk," Witty said.

Greater Accountability Needed

Warner also focused on the lack of backup systems, saying these must be in place. Either an entity like Change has such a system, or perhaps "the whole business model needs to change so that whoever you sign up with, you have a backup in reserve," said Warner. Witty replied that some of Change's customers didn't have backups of their own data, and said UHG also needs to work with providers to help them "have that second pipeline."

Warner said he is eager to work with Wyden and other committee members to address the need for resiliency and backups, saying it is "well overdue. We were just waiting for a crisis like this to happen. We knew it was going to

happen. Now I think we need to act."

Wyden agreed. He noted the Finance Committee has jurisdiction over Medicare as well as the HIPAA Security Rule, "which gives us a chance to look at some of these issues relating to enforcement and standards and accountability" and "a chance to make a link between prevention…and redundancy…in a bipartisan way. There's lots to do and I look forward to working" with committee members.

Warner also noted that, in November 2022, he issued a white paper on cybersecurity policy options that included a chart showing that HHS, the Departments of Homeland Security, Justice and Commerce all have some level of jurisdiction over health care cybersecurity, as do "about 12 different entities."

"This lack of clarity is one of the challenges," Warner said, as is the lack of minimum cybersecurity standards in health care. He asked Witty if he agreed that such standards were needed.

"We're supportive of a direction of travel which moves towards minimum standards," Witty said. "Today, there is a blend of guidance, some standards and others. There needs to be clarity within that." He suggested that "smaller and medium-sized organizations across health care [find it] difficult oftentimes to navigate some of those things. A refreshed view of all of that…minimum standards do make sense."

Warner said standards need to exist "up and down the food chain," as evidenced by the Change breach, which occurred in an entity that was a middle player in the health care system.

Wyden Calls for New Cybersecurity Rules

But Wyden also laid some blame on OCR.

For non-health care entities "regulated by other federal agencies, meeting a baseline of essential cybersecurity standards is a must," Wyden said. But this is "meaningless without strong enforcement."

HHS, Wyden said, "has not conducted a proactive cybersecurity audit in seven years. As it stands, if a company doesn't comply with the relatively meager cybersecurity regulations, fines amount to nothing more than a slap on the wrist."

In his view, "federal agencies need to fast-track new cybersecurity rules for American's private medical records, and the Congress needs to watchdog this every day to make sure that what is getting done is the essentials of protecting patient data."

Wyden added that the breach "is a dire warning about the consequences of too-big-to-fail mega-corporations gobbling up larger and larger shares of the health care system. It is long past time to do a comprehensive scrub of United Health's anticompetitive practices, which likely prolonged the fallout from the hack."

Sen. James Lankford, R-Okla.—noting that he also serves on the Homeland Security Committee—asked Witty to provide him with "any specific ideas" that could be useful in drafting future legislation or in other efforts to help prevent future ransomware attacks, such as "things the FBI could have done better, things that would have been helpful proactively or information that would be helpful." Witty said UHG "would be happy to" come up with suggestions.

Encrypted Files Hampered Provider Notification

Other senators raised problems related to communication, which Witty admitted need attention.

Some providers first learned about the breach, not from UHG, but through the news media, Sen. Todd Young, R-

Ind., said, noting that Tulip Tree Healthcare—a community health center in southern Indiana—was "unable to switch clearinghouses…they indicate it's a time-sensitive process for their billing department, which has two people. And connecting to the new system could put their cyber liability insurance at risk since it hasn't been guaranteed secure."

Tulip Tree had to resort to a "100% paper submission of claims by mail, incurring all kinds of overtime, expenses and significant postage costs for a small health care center that tries to provide the most they can for their patients," Young said.

Young asked Witty if UHG had a notification process in place. "That's a very good question," Witty responded, "and that's one of the areas where I think we need to figure out how to communicate, not just for companies, but for government." Change Healthcare's files were "compromised" and "encrypted, which made it very difficult for us to reach out directly to those clients."

UHG "used everything from our UHG insurance provider bulletin, which goes to about a million physicians across the country; we've used social media; we've sent something like 700,000 emails to a variety of different provider addresses; we've tried to use every channel. We've worked with all of the key medical associations to encourage associations to get the word out to pharmac[ies], to providers and others," Witty said. "We've been running regular, national telephone calls for technology leaders across all of the organizations and encouraging them to spread the word in their region." UHG also encouraged large hospitals to "spread the word."

Still, with all of this effort, "communication to providers…whether it's a cyber situation or a pandemic situation… is an area which repeatedly comes up as an area for opportunity," Witty said.

Young said UHG "will have all manner of lessons learned, including that there may be limitations under existing law to being able to respond to these sorts of attacks and to serve your clients optimally. To the extent those lessons are learned, I ask that you communicate that information to my office and to this committee so that we might consider changing the law."

'Cascading Series of Crises' for Hospital

Sen. Tom Carper, D-Del., said the government has a role to play in securing health data and preventing ransomware attacks, and also asked Witty what tasks the government should undertake.

Witty said there were "maybe two areas" for government action, such as establishing "minimum standards" and determining what "the right level of system protection and redundancy is to try and guard against the impacts of future attacks. And then the second is to see what further can be done, what more can be done, to reduce the attack velocity that is coming at the U.S. health care system from cyber criminals and other possible actors."

As of the date of the hearing, a critical access hospital in Colorado had $1.5 million in outstanding payments, Sen. Michael Bennett, D-Colo., told Witty.

"That's half of their total monthly revenue. Their ability to pay their doctors and nurses and other staff is at risk as a result of this," Bennett added. Providers, "already operating on a shoestring," are "two-to-three months away from their normal cash flow." Good Day Pharmacy in Loveland, Colo., has had to charge patients "the cash price of medications…some of which cost over a $1,000, for over 30 days." Some patients, unable to afford the charges, "haven't gotten their medicine; they've been left empty-handed as a result of that," he said.

The attack, added Bennett, "kicked off a cascading series of crises," revealing "some deep vulnerabilities in the core of our health care system, and Colorado practices and hospitals have been left to pick up the pieces covering the cost of someone else's cybersecurity failure."

Witty: We Need Help

Bennett asked Witty how such a devastating breach could be prevented in the future.

Witty said this was "a very good question."

UHG is "clearly trying to take our responsibility…and also trying to learn from [the breach]. We want to make sure we share all of those learnings. We're trying to be as open as we can be on the things we're learning. We'll continue to do that as our investigations continue to pursue any other understandings here," Witty said.

However, he also stressed that the situation is worsening and problems are bigger than anything UHG can change alone.

"The attacks we're under are sustained. They are going up…not going down. The attacks are becoming more and more sophisticated, and the levels of technology that we're going to need to protect against those attacks will continue to have to be elevated," Witty said. "And that's gonna be a challenge for many participants in the system to keep up with the pressure."

As a result, "it's also important that we focus on how we reduce the attack rate and making sure that the numbers of attacks which come into the health system, and more broadly into the country, begin to drop," Witty added.

"The probability of other breaches in other parts of the health care environment must be high given the pressure that the system is under," he said.

1 United States Senate Committee on Finance, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," full committee hearing, May 1, 2024, https://bit.ly/3xYtvMf.
2 "Theresa Defino, "UHG's Breach Response May Prove Enlightening for Others," *Report on Patient Privacy* 24, no. 5 (May 2024).
3 Andrew Witty, "Hacking America's Health Care: Assessing the Change Healthcare Cyber Attack and What's Next," testimony before the U.S. Committee on Finance, May 1, 2024, https://bit.ly/3QyUvbP.