FOR IMMEDIATE RELEASE
May 1, 2024

Contact: Keith Chu 202) 224-4515

Wyden Hearing Statement on Change Healthcare Cyberattack and UnitedHealth Group's Response

As Prepared for Delivery

This morning the Finance Committee examines the Change Healthcare hack that nearly brought the nation's health care system to a standstill six weeks ago. Joining the committee is Andrew Witty, the CEO of UnitedHealth Group, which owns Change Healthcare.

I'll put things in perspective. Last year, UHG generated $324 billion in revenue, making it the 5th largest company in the U.S. Overall, the company touches 152 million individuals across all lines of business – insurance, physician practice, home health, and pharmacy. With its profits, UHG has purchased dozens of other health care companies and is the largest purchaser of physician practices. This corporation is a health care leviathan.

I believe the bigger the company, the bigger the responsibility to protect its systems from hackers. UHG was a big target long before it was hacked. The FBI says that the health care industry is the number one target of ransomware. It's obvious why.

Change Healthcare processes roughly 15 billion health care transactions annually, and a third of Americans' patient records pass through its digital doors.

Change specializes in moving patient data from doctor's office to doctor's office, or to and from your insurance company. That means medical bills that are chock full of sensitive diagnoses, treatments, and medical histories that reveal everything from to abortions to mental health disorders to diagnosis of cancer to sexually transmitted infections.

Military personnel are included in this data. Leaving this sensitive patient information vulnerable to hackers, whether criminals or a foreign government, is a clear national security threat. I don't think it's a stretch the impact here rivals the 2015 hack of government personnel data from the Office of Personnel Management, which the FBI called a "treasure trove" of counterintelligence information for foreign intelligence services.

UHG 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. The failures of CEOs like Mr. Witty, who months in can't figure out how many people have had their data stolen, validate the FBI's warning.

In the wake of the hack, United essentially disconnected Change from the rest of the health care system. It took weeks for Change to get back online, leaving health care providers in a state of financial bedlam. Doctors and hospitals went weeks delivering services but without getting paid. Insurance companies couldn't reimburse providers. Even today, key functions supporting plans and providers, including sending receipts for services that have been paid and the ability to reimburse patients for their out of pocket costs, are not back up and running.

Small providers – particularly mental health providers – have been left holding the bag, stuffing envelopes with paper claims, and unable to get straight answers on how long the outage will last. And patients are bearing the brunt of it. Prescriptions went unfilled, patients were stuck at the hospital longer than needed, and Americans are still in the dark about how much of their sensitive information was stolen. The credit-monitoring service United offered these patients is cold comfort.

The Change Healthcare hack is considered by many to be the biggest cybersecurity disruption to health care in American history. It is Exhibit A for my case that tough cybersecurity standards are necessary to protect critical infrastructure – and patients – in this country. HHS does not require health care providers, payers or health care clearinghouses like Change to meet minimum cybersecurity standards, unlike industries regulated by other federal agencies.

Meeting a baseline of essential cybersecurity standards is a must, but is meaningless without equally strong enforcement. HHS has not conducted a proactive cybersecurity audit in seven years. As it stands, if a company does not comply with existing cybersecurity regulations, the fines amount to nothing more than a slap on the wrist.

Federal agencies need to fast track new cybersecurity rules for Americans' private medical records and Congress needs to watchdog this every day to make sure everything possible is done to protect patient data.

Finally, the Change hack 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 UHG's anti-competitive practices, which likely prolonged the fallout from this hack. For example, Change Healthcare's exclusive contracts prevented more than one third of providers from switching clearinghouses, even though Change's systems were down for weeks.

Accountability for Change Healthcare's failure starts at the top. Before this hearing, I asked U-H-G which members of its board have cybersecurity expertise. UHG pointed to NCAA President Charlie Baker, who signed some technology-related legislation into law years ago when he was governor of Massachusetts. Mr. Baker is certainly an expert on basketball, but UHG needs an actual cybersecurity expert on its board.

Mr. Witty owes Americans an explanation for how a company of UHG's size and importance failed to have multi-factor authentication on a server providing open door access to protected health information, why its recovery plans were so woefully inadequate and how long it will take to finally secure all of its systems.

I'm hopeful that today's hearing can mark the beginning of the Finance Committee's work to make meaningful improvements in America's cybersecurity on a bipartisan basis. I encourage all members to focus on the subject at hand. It's an important topic and there is much to discuss.

###