Today's hearing is about what likely is the most consequential cyber-attack in health care history.

How could something like this happen. How did consolidation in the health insurance industry reach such a state that a single ransomware attack on one company can cripple the flow of claims and payments for months?

Change Healthcare, a UnitedHealth subsidiary acquired in 2022 and was subject to the cybersecurity attack. It operates the largest Electronic Data Interchange clearinghouse in the nation.

Roughly 50 percent of U.S. medical claims pass through or touch Change's clearinghouse, making it an essential link between providers and insurers.

A single company having this much of the medical claims processing market share makes them a large target for bad actors.

It is even more astounding when you consider that the attack itself reportedly occurred using "compromised credentials", without multifactor authentication. This authentication is a pretty standard defense to prevent cyberattacks.

I am concerned about the patients who have been affected.

Many patients were left having to pay large amounts of money out of pocket for their medications because the pharmacy couldn't process their claims or their copay coupons.

The Marion Family Pharmacy in Marion, Virginia, in my district, said the biggest effect has been patients not being able to afford their medication without copay assistance cards.

The owner of the pharmacy even said, and I quote, "We've got people walking away from diabetes medicines, antipsychotics, and ADHD medications."

One specific example was a patient having to pay $1,100 for medication since the pharmacy was not able to process her copay assistance card due to the cyberattack.

United is contractually obligated to pay for these medications, yet patients are still paying premiums and forced to either walk away, pay large sums of money for their medications and even have to borrow money from friends, family, or interest-bearing cash advances on their credit cards.

Providers were also deeply affected by this cyberattack.

In the initial phase, providers were left in the dark as to why United stopped processing claims.

There was deep uncertainty about how to get their claims to flow uninterrupted, the loan program was minimal and restrictive, while bringing on many unrecognized expenses such as switching clearinghouses and managing prior authorization.

It's particularly troublesome because doctors are worried about keeping their practices open, United, by shutting down its clearinghouse and effectively stopping all payments on claims, making it more difficult to continue providing services.

One suburban Philadelphia physician who runs a $6 million-a-year practice was offered only $3,300 by UnitedHealth's emergency loan program. She might have to sell her practice.

How many millions of dollars of interest alone has United made from holding on to money that it would otherwise have had to pay to providers and for patients?

How many millions of surgeries, treatments, and prescriptions were delayed, or worse, cancelled?

I understand the substantial task United is facing while dealing with the fallout from the cyberattack, but I look for an explanation on how they did not have a backup plan.

If they did have one, it obviously failed - resulting in the federal government having to step in.

Additionally, we do not know how many patients had their health information breached.

Last week, United conceded that the personal healthcare information and data of a "substantial proportion" of Americans has been stolen.

At this hearing, I hope we can get an understanding of just how many Americans fall within United's definition of "substantial proportion."

Even though United paid the ransom, we now have reports that cyber criminals are releasing patient information, billing records, and other personal health data held by UnitedHealth Group onto the dark web anyway.

I am hopeful this hearing will shed light on these issues so we can understand the full picture.

I can assure you that this subcommittee will be watching closely. I am always willing to hold follow-up hearings if needed.