Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Hearing on "Examining the Change Healthcare Cyberattack"

May 1, 2024

We are here because a cyberattack on UnitedHealth Group's Change Healthcare resulted in a prolonged disruption to our health care system earlier this year.

The cyberattack has caused serious harm to patients, providers, and pharmacies. Change Healthcare's platforms are reportedly involved with one of every three patient records – processing 15 billion transactions every year. As a result of this cyberattack, health care providers have suffered tremendous delays in reimbursements. Patients have also been forced to either front out-of-pocket expenses for their medicine or to delay treatment because pharmacies have been unable to process claims.

After Change Healthcare's systems were taken offline on February 21st, UnitedHealth Group failed to provide clarity as to when its systems would be online again. In fact, UnitedHealth's status updates repeated the same language for over a week that the disruption was, "expected to last at least through the day." This frustrated the ability of providers and pharmacies to conduct their day-to-day operations and decide whether to use alternative systems in the meantime. Now, over two months later, the system is still not completely back to where it was and there is a backlog of claims that need to be submitted and processed.

The delayed restoration and lack of communication from UnitedHealth Group about a central part of our health care system is unacceptable. We would not accept a bank or internet service suddenly being offline for weeks or months without a clear end in sight. And it is wrong that health care providers, pharmacies, and patients continue to bear the brunt of a failure by a corporation that earned $371 billion last year to either prevent or quickly remedy this situation.

I am sure that we will be hearing from Mr. Witty about all the various things that UnitedHealth has done since the cyberattack to help providers, patients, and other payers. But the bottom line is that UnitedHealth's data security practices were woefully inadequate. The company also did not have a plan in place to quickly recover from such an attack and to minimize the damage to everyone impacted. While it is true that the largest health care company in the country has since dedicated resources to clean up its mess, it feels like too little too late for all those who have been harmed.

To make matters worse, we still do not know the full extent of the damage from this cyberattack. Even if all providers, pharmacies, and patients are made whole and the system returns to normal, huge volumes of protected health information appear to be in the hands of

hackers. As UnitedHealth announced last week, this data breach could affect the privacy of, "a substantial proportion of people in America."

As part of our work on comprehensive federal consumer data privacy and security legislation, the Committee has held numerous hearings highlighting the importance of companies adopting strong privacy and data security protections. So it is extremely frustrating to have one of the largest companies in the world failing to meet its obligation under existing law to adequately protect some our most sensitive personal information. We're talking about sensitive information like our health care status, what medications we take, and what medical services we are provided.

Mr. Witty, this never should have happened and it cannot happen again. UnitedHealth Group must do the hard work of adopting strong data security practices that include protecting against such attacks and adopting plans that minimize the impact of such attacks.

It is going to take a lot of work to untangle this mess. The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services (CMS) have worked very hard throughout this crisis to minimize the damage to essential health programs. HHS's Office for Civil Rights also has lots of work ahead as it examines what went wrong here and the harm caused by the theft and potential release of HIPAA-protected data.

As we learn more about what went wrong, this Committee should examine whether additional guardrails – such as establishing cybersecurity requirements on Medicare contractors – need to be put in place to prevent this from happening again. This hearing is a good start, and I thank Chairs Rodgers and Griffith for holding it. I look forward to working with my colleagues on the issues raised here and, importantly, hearing from Mr. Witty about how to make sure this does not happen again.

Thank you, Mr. Chairman, I yield back.