Committee on Energy and Commerce
Opening Statement as Prepared for Delivery
of
Subcommittee on Health Ranking Member Anna Eshoo

Hearing on "Examining Health Sector Cybersecurity in the Wake of the Change Healthcare Attack"

April 16, 2024

Thank you Mr. Chairman and good morning colleagues. Today we'll discuss the dire need for stronger cybersecurity measures in the health care sector following a major cyberattack on Change Healthcare in February that ground medical claims processing to a halt.

Change operates the largest clearinghouse for medical claims in the United States and reviews 15 billion, with a B, medical claims annually. Its network encompasses more than 900,000 physicians, 118,000 dentists, 33,000 pharmacies, 5,500 hospitals and 600 labs.

Change is a subsidiary of Optum Insight which is owned by UnitedHealth Group, a health care behemoth that among other entities, owns commercial insurer UnitedHealth and PBM OptumRx.

On February 21st of this year, Change disconnected over 100 systems after detecting a cyberattack within its networks that likely compromised sensitive patient data. Effects of the cyberattack reverberated across the country within hours, with hospitals, pharmacies, and physician practices losing up to $1 billion, with a B, dollars a day.

Today, most systems are back online and claims processing is underway again for many providers, but the full impact of the cyberattack remains to be seen. UnitedHealth hasn't confirmed the volume or type of patient data that was compromised. It has been reported up to 4 terabytes of data may have been stolen and there are new, unverified claims that other bad actors also have possession of the stolen data.

On March 13th The Office of Civil Rights at HHS announced it would investigate whether UnitedHealth failed to comply with privacy and security standards under HIPAA. It's good to know that HHS is also working to address the cash flow crunch caused by the attack by offering accelerated and advanced payments. This is very important and obviously helpful.

UnitedHealth was a target because of its size. It's the largest health company in the world by revenue and since the early 2000's, it's been consolidating health care services under its subsidiary Optum. The attack shows how UnitedHealth's anticompetitive practices present a national security risk because its operations now extend through every point of our health care system.

The cyberattack laid bare the vulnerability of our nation's health care infrastructure. The health care sector is a hackers' playground because it offers services people need and handles a massive amount of medical records which sell on the dark web for $60 a pop.

At the same time, health care organizations do not invest in cybersecurity. The average hospital spends six percent of their operating budget on information technology and cybersecurity – a fraction for most health systems grossing millions in revenue each year.

According to the American Hospital Association, cyberattacks against hospitals increased by 57 percent in 2022. About 90% of hospitals have had at least one data breach and 45% of hospitals experienced five or more in a single year. The average data breach costs $11 million resulting from missed revenue and system upgrades. Cyberattacks also put patient lives at risk, delaying needed care and forcing patients to transfer to alternate care settings.

Despite significant increase in cyberattacks perpetrated against the health care sector, a lesson holds true: we spend more money cleaning up a mess after it happens, rather than paying for less inexpensive prevention measures up front.

It's not a question of 'if' a cyberattack will happen. It's a question of 'when.' Health care organizations are long overdue to institute strong cybersecurity measures and enhance data security to safeguard patient information.

What's taken place should serve as a wake up call to the health care sector. So I look forward to hearing from our witnesses today about how reforms can be implemented without further delay.