NEVER ALLOW ANY COMPANY TO STORE YOUR DATA ON A NETWORK OR YOU WILL BE DESTROYED

Mon, 26 Dec 2022 07:46:38, swmof88, [post_tag: never-allow-any-company-to-store-your-data-on-a-network-or-you-will-be-destroyed, category: news]

'biggest medical cyber-attack in history': IT system that holds hospital records of 20million Americans is hit causing cancer delays and ambulance diversions

- **CommonSpirit health has admitted to suffering 'IT issues' due to a cyberattack**
- **The fourth largest health system in the country is facing disruption in units**
- **It was not clear how many of the 140 hospitals across 21 states are affected**

By Luke Andrews Health Reporter

The medical records of up to 20million Americans may have been leaked in what could turn out to be the biggest medical cyberattack in US history.

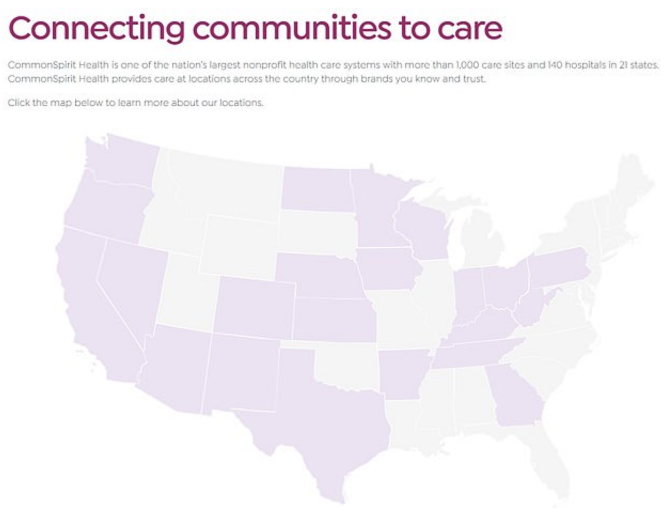
CommonSpirit Health — the fourth largest health system in the country — was the target of a major IT ransomware attack this week.

It is not clear how many of the 140 hospitals across 21 states are affected, but the hack has already led to cancer appointments being cancelled and ambulances diverted.

Among those affected are the Virginia Mason Medical Center in Washington — the second best in the state — and MercyOne Medical Center in Iowa.

IT experts today warned it may be the 'biggest' ever to cyber attack on a medical system in the US.

Pictured above is the MercyOne hospital in Iowa, one of the facilities that has been affected in the ransomware attack. Operations are being cancelled for patients



Connecting communities to care

CommonSpirit Health is one of the nation's largest nonprofit health care systems with more than 1,000 care sites and 140 hospitals in 21 states. CommonSpirit Health provides care at locations across the country through brands you know and trust.

Click the map below to learn more about our locations.

Shown above are the states where CommonSpirit Health operates. It is not clear which units have been affected, but hospitals in Tennessee, Iowa and Washington have all reported issues

© Cushwake Properties via Vimeo

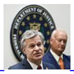
Pictured above is the HQ for CommonSpirit Health in Chicago, Illinoise. The system serves more than 20 million patients and has 140 hospitals across 21 states

A CommonSpirit spokesman admitted this week that electronic health records — which hold patient data — and other systems had been taken offline.

They added: 'As a result of this issue [the IT attack], we have rescheduled some patient appointments.

'Patients will be contacted directly by their provider and/or care facility if their appointment is impacted.'

-

- Personal data of celebrities including Jeremy Clarkson, the...  Three Iranians are charged with mounting cyber-attacks on...

Biden warns there is 'evolving intelligence' Russia will hit US with cyberattacks

The Biden administration is warning about the danger of Russian cyber attacks on U.S. businesses or infrastructure amid the war in Ukraine – and warning the U.S. will respond.

A White House fact sheet from March highlights the potential for Russia to launch 'malicious cyber activity' in response to sanctions the U.S. imposed on Russia since it invaded Ukraine last month – and the administration is revealing it has seen 'preparatory activity.'

'I think the President was very clear. We're not looking for a conflict with Russia. If Russia initiates a cyber attack against the United States, we will respond,' said Senior White House cybersecurity official Anne Neuberger, who briefed reporters at the White House.

The White House is not saying such an attack has occurred since the new sanctions, a matter that has surprised some Russia observers. But Moscow may be taking steps to prepare for such an event.

'There is now evolving intelligence that Russia may be exploring options for potential cyberattacks,' according to the fact sheet.

Patients affected include Kathy Kellog, from Washington, who had her operation to remove a cancerous tumor from her tongue delayed by at least five days.

Her husband Mark told KING-TV: 'Everything we do today is all on a computer, and without it you're back to the stone age writing on a tablet.'

The hospital they were attending — Virginia Mason Medical Center — is one of several that took systems offline due to the cyberattack.

The CHI Memorial Hospital in Tennessee also had to delay operations, and the St Michael Medical Center in Washington delayed critical procedures such as CT scans checking for brain bleeds.

No one has claimed responsibility for the attack at present.

But earlier this year President Joe Biden warned Russia would likely step-up its cyberattacks on US businesses and infrastructure over the Ukraine war.

He has vowed that America will respond if any attacks are linked back to the Kremlin.

Brett Callow, a threat analyst with cybersecurity provider Emsisoft, said if all the health system's hospitals were affected the attack could be the 'most significant on the healt hcare sector to date'.

The IT expert has helped curb at least 15 ransomware attacks on health systems in the US this year.

Four-fifths of these resulted in data being stolen from hospitals, he said.

He warned these often 'represent a risk to the lives of patients' due to disruption to ambulance services and operations.

The delays caused, he said, impacts the 'long-term patient outcomes' — or chance of recovering from the procedure.

No patient deaths have been explicitly linked to ransomware attacks in America so far.

But last year a hospital in Alabama was sued after it was alleged a software hack led to the death of a baby girl.

Mother Teiranni Kidd claimed the eight-minute delay in getting a specialist to unwrap the umbilical cord around her daughter's neck caused by the hack left her baby with brain damage that she later died of. She said the hospital did not tell her its network was down when she arrived to give birth.

Sources in the CommonSpirit health system confirmed the attack was from ransomware, NBC News reports.

This is a malicious type of software that blocks access to patient systems, saying it will only re-open them after receiving a payment.

It is not clear who is behind the attack, or how it occurred.

It began on Monday, but was yet to be resolved by Friday this week.

The biggest ever in US history was in September 2020 when a ransomware attack arrested services at all 250 facilities — and 28 hospitals — owned by Universal Health Services.

But the attack on CommonSpirit — which has more than 700 facilities — could be the largest yet, depending on how many centers were affected.

In 2020, the FBI and other federal agencies warned that they had credible information that cybercriminals could unleash a wave of data-scrambling extortion attempts against U.S. hospitals and health care providers.

That’s because ransomware criminals are increasingly stealing data from their targets before encrypting networks, using it for extortion.

They often sow the malware weeks before activating it, waiting for moments when they believe they can extract the highest payments.

Health care is classified by the U.S. government as one of 16 critical infrastructure sectors Health care providers are seen as ripe targets for hackers.

If patient data is accessed, health care providers are required by law to notify the Department of Health and Human Services.