An ‘unprecedented’ hospital system hack disrupts health-care services

Washington Post
Analysis by Tim Starks
with research by McKenzie Beard
October 6, 2022 at 7:23 a.m. EDT
https://www.washingtonpost.com/politics/2022/10/06/an-unprecedented-hospital-system-hack-disrupts-health-care-services/

Chicago-based, CommonSpirit Health faced a cyber security attack in the past week.

Occurred on October 4, 2022. Updated statement on October 5. Unsure current status. Not releasing many details. Here’s what we know:

CommonSpirit Health has 140 hospitals and more than 1,000 care sites in 21 states. Facilities in Iowa, Nebraska, Tennessee and Washington were among those enduring disruptions.

- The outage appeared to be affecting medical sites nationwide under the CommonSpirit Health operating umbrella, including North Dakota, Nebraska, Tennessee, Texas and Iowa, based on media reports from those states.
- The original online statement read. “Our facilities are following existing protocols for system outages and taking steps to minimize the disruption.”
- The chain declined to comment further, but signs point to a ransomware attack, during which hackers encrypt victim systems and demand payment to unlock them.

Consequences of the CommonSpirit Health incident:

- Some IT systems and records have had to go offline
    - Paper charting
    - No access to patient records for health histories
    - Slowing everything down, very inefficient
- No access to scheduling systems
    - Using paper
    - Checking patients off as the arrive
    - Unable to call patients to cancel
    - Patients arrive for appointments scheduled for months, and cannot be seen
    - Rescheduling appointments
- Hand writing prescriptions
- Diverting ambulances
- Delayed critical medical procedures, including a CT scan to check on a brain bleed
- Healthcare workers told the Tacoma News Tribune that “the disruption was having serious impact on normal functions such as charting, lab results reporting, history gathering, obtaining records on allergy information and more.”

There have been a couple reports that cyberattacks on hospitals have cost lives.

- A lawsuit that a woman filed against an Alabama hospital last year alleges that a ransomware attack led to the death of a 9-month-old child because of equipment that wasn't working.
- In 2020, a German hospital under ransomware attack turned away a patient who later died. Prosecutors looked at filing charges against the hackers, but ultimately concluded it wasn't the decisive factor.

Past Attacks:

- In perhaps the most sweeping hospital cyber incident outside the United States, the massive WannaCry ransomware attack that affected 150 countries hampered the U.K. health system. The 2017 incident disrupted 80 hospitals, led to the cancellation of 19,000 appointments and cost it more than $100 million.

Ransomware Trends 2021 - HHS

https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf

- Health Sector Cyber Security Coordination Center (HC3) has tracked a total of 82 ransomware incidents impacting the healthcare sector worldwide so far this calendar year, as of May 25, 2021. (report released in June)
  - 48 of these ransomware incidents (or nearly 60%) impacted the United States health sector.
- 5 Major Ransomware ”actors” globally
- Survey of HPH organizations worldwide between January and February 2021:
  - 34% of healthcare organizations were hit by ransomware in the last year.
  - 65% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack.
  - 44% of those whose data was encrypted used backups to restore data.
  - 34% of those whose data was encrypted paid the ransom to get their data back
  - 93% of affected HPH organizations got their data back, but only 69% of the encrypted data was restored after the ransom was paid
- The average ransomware payment for the HPH sector is $131,000.
  - The average bill for rectifying a ransomware attack – considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. – was $1.27 million.
  - While this is a huge sum, it's also the lowest among all sectors surveyed

Preparedness Strategies:

- The American Hospital Association's national adviser for cybersecurity and risk said it's important for hospitals to have a plan for when an attack happens.
- Downtime procedures need to be in effect that would compensate for lack for access to electronic health records and other medical technology that may become unavailable
- Require multi-factor authentication for remote access to OT and IT networks.
- Enable strong spam filters to prevent phishing emails from reaching end users. Filter emails containing executable files from reaching end users.
- Implement a user training program and simulated attacks for spear phishing to discourage users from visiting malicious websites or opening malicious attachments, and re-enforce the appropriate user responses to spear phishing emails.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing URL block lists and/or allow lists.
- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner. Consider using a centralized patch management system; use a risk-based assessment strategy to determine which OT network assets and zones should participate in the patch management program.
- 3-2-1 Backup Rule
  - Maintain at least 3 copies of your data
  - Keep 2 copies stores in separate locations
  - Store at least 1 copy at an off-site location
- Many more strategies listed in the HHS resource
- Overall, the health-care sector needs help from law enforcement to track down and punish culprits

*** DHS will require companies to address ransomware in their cyber-preparedness, or face penalties

Resource:

https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf