MedStar paralyzed as hackers take aim at another US hospital

March 29 2016, by Jack Gillum, David Dishneau And Tami Abdollah

A sign designates an entrance to the MedStar Georgetown University Hospital in Washington, Monday, March 28, 2016. Hackers crippled computer systems at a major hospital chain, MedStar Health Inc., on Monday, forcing records systems offline for thousands of patients and doctors. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems. (AP Photo/Molly Riley)

Modern medicine in the Washington area reverted to 1960s-era paper systems when one of the largest hospital chains was crippled by a virus

that shuttered its computers for patients and medical staff.

The FBI said it was investigating the paralyzing attack on MedStar Health Inc., which forced records systems offline, prevented patients from booking appointments, and left staff unable to check email messages or even look up phone numbers.

The incident was the latest against U.S. medical providers, coming weeks after a California hospital paid ransom to free its infected systems using the bitcoin currency. A law enforcement official, who declined to be identified because the person was not authorized to discuss an ongoing investigation, said the FBI was assessing whether a similar situation occurred at MedStar.

"We can't do anything at all. There's only one system we use, and now it's just paper," said one MedStar employee who, like others, spoke on condition of anonymity because this person was not authorized to speak with reporters.

There were few signs of the attack's effects easing late Monday, with one employee at Georgetown University Hospital saying systems were still down, and saying some managers had to stay late and come in early because of the disruptions.

A woman walks out of the MedStar Georgetown University Hospital in Washington, Monday, March 28, 2016. Hackers crippled computer systems at a major hospital chain, MedStar Health Inc., on Monday, forcing records systems offline for thousands of patients and doctors. The FBI said it was investigating whether the unknown hackers demanded a ransom to restore systems. (AP Photo/Molly Riley)

Company spokeswoman Ann Nickels said she couldn't say whether it was a ransomware attack. She said patient care was not affected, and hospitals were using a paper backup system.

But when asked whether hackers demanded payment, Nickles said, "I don't have an answer to that," and referred to the company's statement.

MedStar operates 10 hospitals in Maryland and Washington, including

the Georgetown hospital. It employs 30,000 staff and has 6,000 affiliated physicians.

Dr. Richard Alcorta, the medical director for Maryland's emergency medical services network, said he suspects it was a ransomware attack based on multiple ransomware attempts on individual hospitals in the state. Alcorta said he was unaware of any ransoms paid by Maryland hospitals or health care systems.

"People view this, I think, as a form of terrorism and are attempting to extort money by attempting to infect them with this type of virus," he said.

Alcorta said his agency first learned of MedStar's problems about 10:30 a.m., when the company's Good Samaritan Hospital in Baltimore called in a request to divert emergency medical services traffic from that facility. He said that was followed by a similar request from Union Memorial, another MedStar hospital in Baltimore. The diversions were lifted as the hospitals' backup systems started operating, he said.

Some staff said they were made aware of the virus earlier, being ordered to shut off their computers entirely by late morning. One Twitter user posted a picture Monday he said showed blacked-out computer screens inside the emergency room of Washington Hospital Center, a trauma center in Northwest Washington.

Monday's hacking at MedStar comes one month after a Los Angeles hospital paid hackers $17,000 to regain control of its computer system, which hackers had seized with ransomware using an infected email attachment.

Hollywood Presbyterian Medical Center, which is owned by CHA Medical Center of South Korea, paid 40 bitcoins—or about $420 per

coin of the digital currency—to restore normal operations and disclosed the attack publicly. That hack was first noticed Feb. 5, and operations didn't fully recover until 10 days later.

Hospitals are considered critical infrastructure, but unless patient data is affected, there is no requirement to disclose such hackings even if operations are disrupted.

Computer security of the hospital industry is generally regarded as poor, and the federal Health and Human Services Department regularly publishes a list of health care providers that have been hacked with patient information stolen. The agency said Monday it was aware of the MedStar incident.