

FBI investigating cyber attack at MedStar Health

By **Andrea K. McDaniels and Ian Duncan** · **Contact Reporters**

The Baltimore Sun

MARCH 28, 2016, 8:27 PM

Hackers attacked the computer system at **MedStar Health** on Monday, forcing thousands of employees in the state's second-largest health care provider to resort to paper medical records and transactions.

The nonprofit, which operates 10 regional hospitals, quickly shut down all computer system interfaces to prevent a computer virus from spreading, officials said in a statement. No patient medical records or other information was compromised, they said.

Medstar said all hospitals and clinical facilities remained open, though its 30,000 employees and 6,000 affiliated physicians couldn't log in to the health care system's computer network.

"MedStar's highest priorities are the safety of our patients and associates and confidentiality of information," the nonprofit said in its statement. "We are working with law enforcement, our IT and Cyber-security partners to fully assess and address the situation."

The **FBI** is helping with the investigation but the agency declined to provide details.

"There's been a suspected cyberattack," said Baltimore FBI spokesman David Fitz. "We're assisting."

Officials with another major health care provider, **University of Maryland Medical Center**, said they put in place added layers of security protection in response to the MedStar outage.

"Unfortunately in today's business environment, IT systems are at risk from cyber criminals intent on causing disruption, financial harm and data espionage," the hospital system said in a statement. "The healthcare industry is not exempt from these risks."

Ted Harrington, a partner at Baltimore computer security company Independent Security Evaluators, said the attack could affect patient care. His company has studied hospital security and recently published a report on the vulnerability of medical devices and databases to cyberattack.

"Without access to that patient data they can't administer care with the same level of effectiveness," Harrington said. "Lack of availability does have implications for patient health."

While some MedStar services weren't available Monday, doctors at its hospitals, including **Union Memorial**, **Franklin Square Medical Center** and **Good Samaritan** continued to see patients despite the attack.

Radiation oncology services at University of Maryland **St. Joseph Medical Center** are contracted through MedStar Health. The department canceled 36 appointments after 10 a.m. Monday and all day Tuesday because of the outage.

One employee at St. Joseph's radiation oncology department said he showed up to work and could not log on.

"The computers were on, but you couldn't log in," said David Bender, a medical dosimetrist in the department. "You could see your desktop, but nothing would open. If you tried to connect to the Internet, you couldn't do anything."

Bender said workers were told to turn off and unplug their computers. He went home at noon because he said his department could not treat patients without access to records.

"I am shocked because they seem to have really good security," he said of MedStar.

The attack comes as hospitals have become a particular target of so-called ransomware attacks, in which hackers install software on a system that encrypts data so that users can no longer access it.

This is often accomplished by convincing a user in the hospital to open an infected email attachment. The hackers then demand payment — often in the form of hard-to-trace digital currency — in exchange for the key that frees the data.

Hollywood Presbyterian Hospital in California recently paid \$17,000 to regain access to its systems. Last week, two other California hospitals came under attack, as did one in Kentucky, according to computer security reporter Brian Krebs, who runs the website KrebsOnSecurity.

The **American Hospital Association**, a trade group, has advised members on these cyberattacks, which have lasted up to a week.

"Although most security experts and law enforcement personnel will advise against paying the ransom, many companies do pay, particularly if the information encrypted are 'crown jewels' and hard to replace," a lawyer for the association wrote in a recent blog post.

"But it's important to understand there is never a guarantee that you will even get your data back, and the hackers now know you are willing to pay the ransom."

MedStar did not provide more details on the nature of the cyberattack here.

At Union Memorial Hospital in Baltimore, patient Mary Carroll, 45, said she was told by staff that the "entire computer system was down" in the hospital. Computer screens at a nursing station and a monitor in the family waiting area also were blank, said Carroll, whose mother was undergoing open-heart surgery Monday.

Carroll's daughter Latae Single, 28, said the public wireless Internet also was not working. The problems were concerning to her, she said.

"How does that affect the patients? Everything in there is connected to their system," she said. "Maybe that's why they're moving so slow in there, because they're doing everything by paper."

Carroll, who was waiting for her mother's surgery to end, said she planned to ask doctors about the computer problems and any impact they might have on her mother's care.

In the hospital's emergency room lobby, patients waited to be seen. A member of the nursing staff said the emergency room was accepting patients as usual.

At Good Samaritan Hospital in Northeast Baltimore, the computers were down in the emergency department, at the desks of the security guards and nurses in the triage waiting room. The nurses were taking insurance information by hand on what one nurse described as one of the busiest days of the week.

The pharmacy was closed and locked. A sign on the glass doors said: "Systems down. We will reopen Tuesday 3/29/16 @ 8 a.m. We apologize for the inconvenience."

Baltimore Sun reporters Kevin Rector and Tim Prudente contributed to this article.

amcdaniels@baltsun.com

twitter.com/ankwalker

Copyright © 2016, The Baltimore Sun

This article is related to: [Hospitals and Clinics](#), [Healthcare Providers](#), [Cyber Crime](#), [FBI](#), [MedStar Health](#), [Good Samaritan Hospital \(Baltimore\)](#), [Union Memorial Hospital](#)