logo Image not found or type unknown

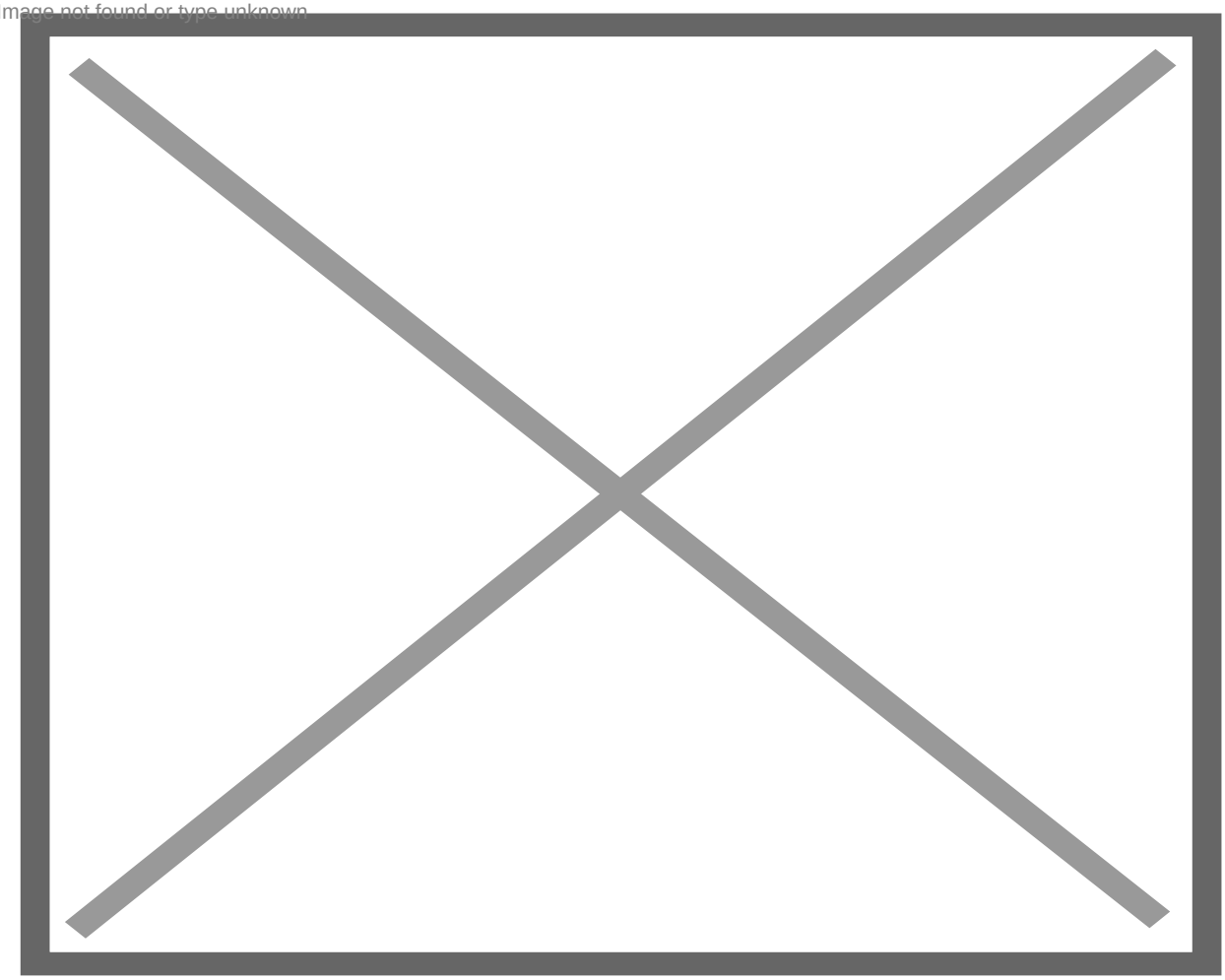
JFL Lost Up to $800,000 Weekly After Cyberattack, CEO Says No Patient or Staff Data Was Compromised

Juan F. Luis Hospital CEO Darlene A. Baptiste says no personal data was stolen in the April cyberattack that forced the hospital offline for months, causing major billing delays, financial losses, and a massive system rebuild now nearly complete.

Health / **Published On October 16, 2025 06:53 AM /**

Ernice Gilbert October 16, 2025

Image not found or type unknown



The April cyberattack that crippled the Juan F. Luis Hospital's electronic systems cost the facility between $750,000 and $800,000 a week, according to CEO Darlene A. Baptiste, who says the breach forced months of manual operations and delayed billing but did not result in any stolen patient or staff data.

Speaking Wednesday during the hospital's "Conversations on Care: Community Dialogue" town hall, Ms. Baptiste detailed how the attack, which occurred on April 26, forced JFL offline for nearly five months and prompted a complete rebuild of its technology infrastructure.

Ms. Baptiste said the hospital was unable to submit electronic bills for months, forcing staff to revert to manual paper billing and resulting in major cash flow delays. "We're thinking somewhere between $750,000 to $800,000 a week that's been lost," she said, before correcting herself to restate: "It's not lost. It's not readily accessible in real time, because we're not submitting our electronic bills in a timely manner."

The CEO acknowledged the toll on staff morale and operations, noting that "being offline for five months has really had an unprecedented impact on us, not only on morale and the energy that is expended to go through it, but the economics."

Recounting the incident, Ms. Baptiste said the attack struck suddenly and required an immediate system lockdown. "I could tell you the exact time — 10:23 that morning — everything shut down. We just locked up. Locked it down," she said.

The attackers gained access through two local servers, exploiting what JFL's IT team later described as an overlooked vulnerability. "We had everything guarded — the windows, the doors, everything was sealed. Everything was tested. But what happened? We had what we call a doggy door, and we didn't protect the doggy door, and they came into there," she explained.

According to Ms. Baptiste, the threat agents infiltrated one drive within the hospital's network but did not compromise personal data. "They found that the threat was within one drive, so they could have had access to everything else, but they just went after this particular drive," she said. "No personal data from patients or staff was compromised during that particular incident."

After the breach, JFL's IT team, working with federal partners and outside cybersecurity experts, performed a full terminal-by-terminal sweep of the system. "All staff went in terminal by terminal and did a clean sweep of everything," Ms. Baptiste said. The federal investigation remains ongoing, with final reports still pending.

During the recovery, hospital operations reverted entirely to manual "downtime procedures" — a paper-based system that replaced the digital records network. "All our systems have been manual since the cyberattack in April 26 of this year," she said.

In September, JFL began its gradual return to digital operations. "Since then, we've had a cutover — it means that we have been in the cloud up until September 17, and we're slowly coming back via clusters that are grouped by specialty," she explained.

At present, 80 to 85 percent of staff have regained access to Meditech, the hospital's electronic health record (EHR) system, while restoration of the financial services and business office clusters is underway.

The cyberattack led to a complete modernization of JFL's IT systems, with significant investments in cloud security, redundancy, and real-time threat monitoring.

"It gives us redundancy, so now we have backups to the backup to the backup," Ms. Baptiste said. "We have partners along with us that also look at having not only the redundancy, but a safety operations center that looks at these threats on a continuum."

These improvements, she explained, ensure constant oversight and reporting. “There are reports that come out on a regular basis that tell us the threats that are readily available in real time, and we can address them based on the trending across the globe,” she said.

While acknowledging the expense, Ms. Baptiste said the overhaul was essential. “It is a pricey endeavor, but we have learned our lesson, literally, the hard way,” she said. “We cannot afford to go down this road again.”

The hospital’s new cloud system also provides greater resilience than its former local servers, offering multiple layers of protection. “God forbid — knocking on everything — we cannot afford to go down this road again,” she said.

The CEO praised the hospital’s employees for keeping services operational despite the crisis. “We had crews that did chart captures and entries, with 15 computer terminals working 24/7 entering and registering patients, keeping operations afloat,” she said. “At some point, we even had four different shifts working around the clock to make sure we had the organization stabilized.”

Working without digital tools was a major challenge, she admitted. “When you’re used to the electronic system and now you have to go to paper, it’s a very heavy lift for our entire staff, nursing and physicians alike,” she said, thanking staff for their endurance and commitment to patient care.

Ms. Baptiste described the cyberattack as a painful but transformative experience that has made the hospital stronger and better prepared. “We found it more prudent for us just to go ahead and rebuild our system, and now we’re coming back stronger. That’s our plan right now, with a heavy ticket price, but it’s well worth it,” she said.

Although the final federal report on the incident has yet to be released, Ms. Baptiste said the hospital’s new security infrastructure provides continuous protection and redundancy. “We cannot afford to go through this again,” she said.

The attack, she added, was a wake-up call that underscored both the importance of cybersecurity and the resilience of JFL’s workforce. “It was a hard but valuable lesson,” she said. “We’ve come out of it stronger.