BECKER'S HEALTHCARE

tigerconnect

Staying Connected During Cyberattacks: The Crucial Impact of CC&C Platforms

Hospitals and healthcare facilities are prime targets in the escalating cyberattacks plaguing the U.S. Hospitals present particularly vulnerable targets because of the vast amount of sensitive hospital data and protected patient information.

Cyberattacks sow chaos by disrupting systems people rely on to deliver care to patients. With patient safety at risk, cyber criminals are betting hospitals will pay the ransom and do so quickly to recover access to their data.

The data is alarming:

- 88 percent of healthcare organizations surveyed by Ponemon report being attacked in the last year.
- Attacks roil payment processing across the industry, as security experts warn that healthcare infrastructure is not sufficiently protected from these criminals.
- Researchers have found that in-hospital patient mortality increases in the aftermath of a cyberattack along with a patient volume decrease of as much as 25 percent in the initial week of an attack as hospital operations slow, impacting patient throughput.

With the increasing frequency and severity of cyberattacks, hospitals must be ready to respond effectively to protect patient safety and maintain operational continuity. Preparation involves more than just securing data; it requires ensuring that communication channels remain open and functional even during a crisis. So, how can hospitals ensure they are ready to face such threats head-on?

Keep everyone connected

Cybercriminals target vital systems and the data they hold. One of the systems targeted is often the electronic health records (EHR). Bottling up the EHR data usually delivers a second blow for those hospitals that rely on EHR chat for communication – it won't work. In those cases, not only is the data unavailable, but hospital staff lose their texting abilities. With other systems – often phone and e-mail – also targeted, staff have no means to stay in contact to keep care flowing to patients.

Hospitals need to proactively create communications systems that are:

- Outside the EHR, though capable of interoperating with it under normal conditions.
- Not reliant on infrastructure housed and facilitated on-premises.
- Capable of mass broadcast, one-to-one and team-based communications in the same system.
- Consistently reliable to use during emergent situations.

Standardizing on a modern, cloud-based clinical communication and collaboration (CC&C) platform creates a new foundation for continuing care delivery while other systems are under siege. When attacks occur – and it increasingly appears that it's a

question of "when" not "if" for many hospitals – a CC&C platform's capabilities enable care teams to stay connected and keep information flowing.

Activate your response immediately

The longer your response takes to organize, the more potential damage to clinical workflows and the more patients are at risk – plus the potential financial repercussions to the institution as patient throughput slows.

A CC&C platform with role- and team-based messaging keeps lines of communication open and enables proactive planning. The entire staff can keep care delivery moving, with text, voice, and video calls through the app on their phones, articulated to the cloud through cellular infrastructure. You can create both broad and targeted contact lists in the app. By doing so ahead of time, you can alert everyone in the hospital of the situation and institute whatever protocols are part of your care continuity plan immediately.

Specialized teams can be constructed ahead of time and activated with a few taps on a phone, utilizing a private channel instrumented through the CC&C platform. An executive crisis team can be activated to deal with the institutional ramifications of the situation before the crisis spreads. The earliest interventions such as working with law enforcement, insurance vendors as well as payment processors might lessen effects before they accumulate.

Likewise, an IT crisis team can be built in the app ahead of time and activated when the moment arrives. It's crucial to protect as many systems and applications as possible from a metastasizing attack. That team can also begin the process of investigation, looking for the vulnerabilities that were exploited by the cyber criminals and plugging those holes. Speed is of the essence and the CC&C platform keeps communication flowing.

And don't forget those outside the four walls of the hospital. A flexible CC&C platform can send secure messages to patient's families and to outside agencies and facilities connected to the hospital. Keeping them informed can head off confusion from external facilities (such as those coordinating patient referrals and transfers) and reputation-damaging rumors developing in the community as the hospital battles the crisis.

Prepare for the worst, and the everyday

Of course, the many benefits of a CC&C platform can help streamline operations absent a cyber-attack. Even on a routine day, a CC&C platform can reduce inefficiencies in how you interact with care teams and your systems. Features like role and team-based communications make it easy to connect everyone involved in delivering care, resulting in greater productivity and better patient outcomes.

Hopefully, you'll never be the victim of a cyberattack. Unfortunately, the reality is that if you care about protecting your organization and your patients' privacy, you need to be prepared for the worst. A CC&C platform is one of the best ways you can ensure care delivery stays moving, especially when you need it most.