

July 19, 2024

## CrowdStrike Technology Outage Causing Global Disruption Across Industries, Including Impacts on Hospitals and Health Systems

*Company says incident is NOT a security incident or cyberattack*

A non-malicious global technology outage that began early Friday morning is continuing to affect many industries and is having varying effects on hospitals and health systems across the country.

The global outage was caused by a faulty software update issued by the cybersecurity firm CrowdStrike, which is widely used by businesses and government agencies that run on Microsoft computers.

“CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts,” the organization posted on its website early today. “Mac and Linux hosts are not impacted. This is not a security incident or cyberattack. The issue has been identified, isolated and a fix has been deployed. We refer customers to the support portal for the latest updates and will continue to provide complete and continuous updates on our website. We further recommend organizations ensure they’re communicating with CrowdStrike representatives through official channels.”

**CrowdStrike’s [webpage](#) includes more information about the issue and workaround steps organizations can take. In addition, view the [Cybersecurity and Infrastructure Security Agency alert](#) on the incident.**

In a statement shared with media this afternoon, AHA National Advisor for Cybersecurity and Risk John Riggi said, “The AHA is in close communication with the hospital field and the federal government about the non-malicious global technology outage that occurred early this morning. While we continue to monitor the situation closely, we are hearing from hospitals and health systems that the impact varies widely. Some have experienced little to no impact while others are dealing directly with some disruptions to medical technology, communications and third-party service providers. These disruptions are resulting in some clinical procedure delays, diversions or cancellations. Impact is also being felt indirectly as a result of local emergency call centers being down. Impacted hospitals are working hard to implement manual restoration of systems and the CrowdStrike patch. Affected hospitals have also implemented downtime procedures to ensure that disruptions to patient care are minimized or avoided to the extent possible.”

## WHAT YOU CAN DO

- Share this Advisory with your IT and cybersecurity teams.
- If you have instances of CrowdStrike in your networks, determine the impact and review your business and clinical continuity procedures.
- Use this opportunity to identify impact and downtime procedures for all internal and third-party life-critical and mission-critical technology, services and supply chain.
- Test cyber incident response and emergency preparedness plans and communication channels.
- Plan for technology disruptions and cyber incidents on a regional basis.
- Be alert to increased phishing emails that may appear related to this disruption.
- Report any clinical impacts that your organization is experiencing to state and local public health officials as appropriate or required. You also may share information with the AHA by emailing Riggi at [jriggi@aha.org](mailto:jriggi@aha.org).

## FURTHER QUESTIONS

If you have further questions, please contact Riggi at [jriggi@aha.org](mailto:jriggi@aha.org). For the latest cyber threat intelligence and resources, visit [www.aha.org/cybersecurity](http://www.aha.org/cybersecurity).