Report on Patient Privacy Volume 22, Number 6. June 09, 2022
IV Pumps Lead List of IoT Devices With Critical Security Flaws

By Jane Anderson

More than half of connected medical devices in hospitals, including the vast majority of ubiquitous IV pumps, contain a known vulnerability that could affect patient safety, service availability or data confidentiality if attacked, a report by cybersecurity firm Cynerio found.[1] The report said one-third of bedside health care Internet of Things (IoT) devices contain an identified critical risk.

"It's a pretty scary finding: Basically more than half of the connected medical and IoT devices contain known critical risks," said Daniel Brodie, Cynerio chief technology officer and co-founder during a webinar explaining the findings.[2] "If you get to a hospital, half of the devices that you're seeing have a critical risk on them."

In addition, Brodie said, close to 80% of the devices with security risks were used in the previous four weeks. "Security risks on these devices can actually affect patient care and patient data, or the ability of a hospital to provide care," he said. "These aren't devices that are stuck in some closet or in some dark, damp basement and aren't really affecting anyone."

This makes updating and securing the devices a real challenge, Brodie explained, because the devices are in constant use. "It means hospitals and health care organizations don't have a lot of slack to roll out those security measures they will want to take care of these risks."