ProcessBolt

Ransomware Attacks Disrupt Care and Can Lead to Patient Fatalities

Hackers are infiltrating the operating systems of hospitals and making critical information inaccessible, often making it impossible to effectively treat patients

Medical Devices Are Creating Risk

56%

Have experienced one or more cyberattacks in the past 24 months involving medical devices

72%

Of providers have reported a high level of urgency to secure IoT/IoMT devices

49%

Of providers do not measure the effectiveness of IoT/IoMT security practices

How is Care Disrupted?

- Critical patient data from EHR is inaccessible
- Medical devices are held hostage and are inoperable
- Key communication channels are shut off
- Sensitive patient information is left exposed

Latest Reported Attacks

- In July 2019, a cyber attack led to a wrongful death case as providers were unable to monitor critical patient information, ultimately leading to a child's death
- In October 2022, an attack on the 4TH largest US health system led to delays in surgeries, patient care and appointments
- In November 2022, cyber criminals held patient data on 9.7 million patients and leaked sensitive information when the ransom was not paid

ProcessBolt enables healthcare organizations to audit and continuously monitor their supply chain and connected medical devices to protect against attacks that compromise patient care

TRUSTED BY TOP HEALTHCARE PROVIDERS

Allina Health

Oregon Health & Science University

omada

Palomar Health

HennepinHealthcare

ProcessBolt, Inc.
processbolt.com
Phone: 612.564.3448
E-mail: info@processbolt.com