HealthManagement.org
Promoting Management and Leadership

ECRI Institute Issues Free Public Resource to Protect Hospitals from Ransomware Attacks

ECRI Institute
The Discipline of Science. The Integrity of Independence.

New guidance gives do’s and don’ts for protecting medical devices from becoming compromised

Ransomware is a form of computer malware that holds systems hostage with a ransom demand. Medical systems are vulnerable to such attacks, which can damage hospital operations and compromise patient care by barring users from accessing critical functions and data.

Today, ECRI Institute, the independent leader in medical device safety and evaluation, announces the publication of a new guidance article, "Ransomware Attacks: How to Protect Your Medical Device Systems." The free resource offers ECRI Institute's independent, unbiased recommendations to help hospitals identify and protect against ransomware attacks.

"With the recent news of nationwide cyberattacks, we thought it was very important to make this information available to the public as quickly as possible," says Juuso Leinonen, project officer, Health Devices Group, ECRI Institute. "Following these recommendations will allow hospitals to minimize impact to normal operations and mitigate the risk of a ransomware infection with your medical devices."

The report provides recommendations for adapting general cybersecurity principles to the particular requirements of medical device systems, including a list of immediate do's and don'ts for quickly responding to emerging threats. This practical guidance will help facilities protect their devices and information in a timely manner.

ECRI Institute has published a number of articles designed to help hospitals respond to cybersecurity threats. These resources provide guidance on topics ranging from ongoing management, strengthening cybersecurity initiatives, and finding future system acquisitions.

At the end of 2016, ECRI Institute launched its Cybersecurity Gap Analysis service to help hospitals and health systems develop a program to protect their medical devices from being used against them in a cyberattack.

"Patching medical devices' software and routinely training staff members about phishing emails are just two aspects of a medical device cybersecurity program; there are many other issues that every hospital has to address," says Robert Maliff, director, Applied Solutions Group, ECRI Institute.

Software management gaps putting patients and patient data at risk is No. 6 on ECRI Institute's annual Top 10 Health Technology Hazards list for 2017; Medical Device Cybersecurity was No. 2 on ECRI Institute's 2016 Top 10 Hospital C-Suite Watch List.

Source & Image Credit: ECRI Institute

Published on : Thu, 25 May 2017