HealthManagement
Promoting Management and Leadership

Protecting cardiac devices against hacking

Medical devices have been targets of hacking for over a decade, and this cybersecurity issue has affected many types of medical devices. In light of recent incidents involving the potential for hacking of cardiac devices (i.e., pacemakers and defibrillators), the American College of Cardiology's Electrophysiology Section Council has published a paper providing suggestions on how medical device cybersecurity can be improved from the standpoint of the manufacturer, government, professional societies, physician, and patient.

In the medical field, cybersecurity refers specifically to the integration of medical devices, computer networks, and software. With the increasing number of medical devices using software, this has "created a new cybersecurity concern in the medical industry — how can we protect devices from intentional harmful interference in their normal functioning?" the paper says.

Hacking attacks pose a potential risk to clinical care, as patients could be harmed by the action of a malignant or inadvertent deleterious change in medical devices' programming by the "hackers".

In August of 2016, Muddy Waters Research LLC released a short-sell report maintaining that cardiovascular implantable electronic devices (CIEDs) manufactured by St. Jude Medical (now Abbott) were at high risk for hacking. The report details two types of cybersecurity breach, using screenshots as evidence: a "crash attack" leading to high rate pacing, and a battery drain attack. The FDA issued a warning letter to Abbott urging the firm to increase cybersecurity based on the Muddy Waters report and the detection of areas of vulnerability in their remote monitoring system.

"A secure system lifecycle approach begins at the conception of device development and continue through manufacture and post-implant monitoring. Cybersecurity needs should also be addressed during both pre- and post-market product testing. As cyber vulnerabilities can emerge quickly, strong post-market processes must be in place to monitor the environment for new vulnerabilities and to respond in a timely manner," the paper explains.

Remote monitoring or interrogation of all telemonitored devices is possible because all CIEDs being followed remotely already communicate with the manufacturer's website. At this time, the paper notes, there is no evidence that one can reprogram a CIED or change device settings in any form. "A more likely scenario is that of a malware or ransomware attack affecting a hospital network and inhibiting communication," the paper says. "In this case, loss of remote communication may prevent timely transmission of a clinical event."

For physicians who manage CIEDs, they should be aware of both documented and possible cybersecurity risks. Systems should be established to communicate updates in these areas quickly and in an understandable way to the rest of the clinical team that manages patients with devices. Policies and procedures for these communications may be informed by the clinic's prior response to FDA device recalls, the paper says.

Amidst rising cybersecurity concerns in the medical industry, the paper notes, the FDA, device manufacturers, and professional societies like the American College of Cardiology and Heart Rhythm Society are actively participating in larger conversations regarding overall risks and how to best protect patients and provide the most effective care.

Source: Journal of the American College of Cardiology
Image Credit: Pixabay

Published on : Wed, 14 Mar 2018