HealthManagement
Promoting Management and Leadership

Patient Safety at Risk: Poor IT Security

Until now and 2021, the total market for cybersecurity technology implemented by U.S. hospitals will expand at a compound annual growth rate of 13.6 percent.
This is according to a new report from Frost & Sullivan which adds that health organisations need to take more action on cybersecurity than implementation of security tools.

The report says that it is not solely patient data at risk but patients themselves as cyberattacks target IT systems with ransomware and other viruses. Says the business strategy firm in its U.S.. Hospital Cybersecurity Market: 2015-2021 report.

Hospitals are being forced into embracing innovation with security strategies as IT security staff shortages and a growing threat to cybersecurity kicks in. The report suggests that the threat to hospital systems could start to impact patient safety as well as data.

It also suggests that the need for innovation in IT security solutions is opening up business opportunities for technology vendors that deal not only in security but general IT development.

"Going forward, all health IT vendors serving the hospital market – and not just vendors of IT security solutions but application vendors as well – must recognise that the increased threat environment demands strong, baked-in security features," said Frost & Sullivan principal connected health analyst Nancy Fabozzi said in a statement.

The benefits of the current insecure environment are that hospitals will become more sophisticated in their demands that will lead to better quality security solutions as companies' offerings are put under greater scrutiny.
"Vendors need to innovate to survive, building or buying advanced functionality and next generation capabilities as the market moves from protecting the walled garden to protecting a vast connected perimeter," said Fabozzi.

Owing to the increased risk of cyber-attacks of every type, especially phishing and ransomware, hospitals are transitioning from their traditional reactive and fragmented approach to protecting privacy and security that is highly dependent on HIPAA compliance to a new approach and mindset that is proactive, holistic, and coordinated, anchored by integrated solutions designed to protect multiple endpoints, Fabozzi added.

Source: Healthcare IT News
Image Credit: Pixabay

Published on : Wed, 10 Aug 2016