David Snyder, MBA, PE, CISSP, CSM
President, 42TEK, Inc.
david@42tek.com
September 27, 2019

Cybersecurity and the Future of Remote Patient Monitoring

How will you ensure cybersecurity for remote patient monitoring systems?

Several trends are driving increased interest and adoption for using network-connected medical devices outside the clinical environment to diagnose, monitor, and treat patients. These include:

- an aging population living longer, often with multiple chronic illnesses
- looming shortages of doctors and nurses
- incentives to reduce hospital readmissions
- increased availability of remote patient monitoring equipment
- availability of reimbursement codes for remote monitoring equipment and for clinicians to have telemedicine appointments and review data from remote monitoring

Best practices have emerged for making sure network-connected medical devices are designed, built, and operated with cybersecurity in mind, but this has largely been for individual devices and for clinical networks to which these devices are connected. Now, we are starting to see "systems of systems" consisting of multiple devices connected to home networks and mobile phones.

Home networks and mobile phones

- vary widely in what is connected
- vary in how well they are patched and updated
- usually are not managed by information technology professionals
- are unlikely to have the level of cybersecurity protection found in hospitals and clinics (e.g., network segmentation, logging, intrusion detection, etc.)
- may include vulnerable devices on the same network as medical devices

Healthcare delivery organizations and patients need guidance on how to make sure home networks and mobile phones are secure and network-connected medical devices outside the clinical environment are

- integrated and installed securely
- maintained securely with updates and patches
- monitored for indications of abnormal behavior that may indicate device failure or compromise

This workshop will explore

- similarities and differences between network-connected medical devices in clinical settings versus residential environments
- challenges facing clinicians and healthcare delivery organizations with respect to ensuring cybersecurity for remote patient monitoring devices
- best practices for cybersecurity through the entire lifecycle of remote patient monitoring devices, from concept and design, through development, testing, deployment, operations, maintenance, repair, replacement, and decommissioning