Word Count: 808
Reading Time: 3.2 minutes

HOSPITALS, HOSTAGE, RANSOM

How Do Those Words Fit Together?

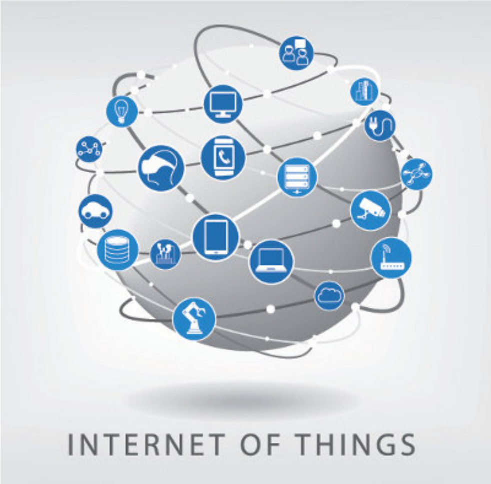
It's been all over the news … hospitals being hacked, data held hostage and ransom paid to the perps. Hollywood Presbyterian Medical Center and MedStar Health in D.C. are two recent victims that have been prominently in the press and paid significant dollars to cyber bandits.

Certainly, access denied to sensitive patient data in the hands of criminal cyber-attackers is bad enough. Patient privacy is invaded and healthcare staff is hamstrung in the absence of patient treatment and status records. People with serious health issues could be denied care.

What though would be the real-time impact of internet muggers taking control of medical devices that monitor vital signs and deliver drugs? Smart medical devices are more and more becoming the norm. And each has an IP address which raises the security stakes even higher. A cyber-assailant who successfully acquires the IP address, makes the device fair game for hacker control … and financial demands to take action to back off.

Traditional technology networks are generally vulnerable and lucrative to attack. Small to medium-size hospitals are marked as primary ransomware targets because their security infrastructure is often lacking. Two events are likely to result in increased exposure and invasion of medical devices by the bad guys:

1. Hospital leadership is becoming more alert and responsive to beefing up their cyber-security and backup of files making it more difficult to be compromised. That will have a negative (positive!) impact of decreased profitability for cybercriminal actors.
2. The accelerating proliferation and interconnectivity of smart medical devices, with yet to be developed safeguards against hacking, are likely to become attractive targets.



That means that the Internet of Things (I0T) is something that will require increased attention by hospitals to prevent patients' being denied critical monitoring or required medications. By 2025, according to a **McKinsey report**, remote monitoring with smart devices could create as much as $1.1 trillion a year in value by improving the health of people with chronic diseases.

Another driver of the adoption of IoT by the healthcare community is its value in opening new ways to create value from information. That is increasingly critical given the growing focus on value-based care now shifting to a compensation model where providers are rewarded financially based on patient outcomes rather than healthcare provider activities, e.g. tests, visits, procedures performed, etc. **Click Here** for a comprehensive report on how IoT is transforming medical technology.

So, adoption of IoT is on a fast-track. New networks are being introduced to handle the increased internet traffic driven by IoT - including that attributable to smart medical devices.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

FDA

STERIS

Hospitals Have Allies

NIST: Earlier this year, the National Institute of Standards and Technology (NIST) announced plans to release new guidance for strengthening hospital cybersecurity.

The objectives of the imminent set of best practices are to help healthcare organizations become more penetration-resistant, more effective at limiting damage attackers can inflict and ultimately better able to withstand cyberattacks.

FDA: The Food and Drug Administration issued a warning about hackable medical devices. The first device to receive such a warning is an infusion drug pump used by hospitals nationally. The Agency **issued a safety notice** that “strongly encourage[s]” hospitals to discontinue their use of the pump.

The FDA voiced concern that smart medical device products, which are often connected to the Internet and hospital networks, can be hacked, affecting their safety and effectiveness and revealing the data they carry.

The **guidance** recommends manufacturers of medical devices monitor, identify and respond to cybersecurity vulnerabilities as part of routine post-market surveillance of their products. They would be required to report some of that information back to the FDA.

Next Steps, Interim and Long Term

Clearly a collaborative effort by healthcare facilities, medical device manufacturers and regulatory authorities will be the optimum long term solution to minimizing hacking of smart medical devices.

In the interim, hospital leadership must continually become more diligent in identifying network vulnerabilities and taking steps to remedy the weaknesses through increased cybersecurity and aggressive data backup protocols.

A simple, affordable and immediate “fix” that hospitals can implement is the acquisition of refurbished medical equipment rather than the purchase of the latest models. Refurbished equipment meets all of the performance requirements of a given device. But without all the interconnectivity bells and whistles of the most recent equipment offerings, it is not a candidate to be hacked.

Consider sterilizer processing equipment as an example. Whether new or refurbished, sterilizers and washers must meet the same pressure, temperature, steam saturation and time performance requirements. The difference between new and refurbished is that the former may be compromised by cyber bandits. Refurbished equipment can not be hacked … and at a cost to hospitals about 50% of the new.