Security standards back healthcare mobility

EE Times, 30th August, 2011

Circulation: 67,000

Mobility tools are welcome facilitators to a better healthcare delivery system, but the information they contain must be kept safe and secure, says IEEE senior member and founder of Biomedical Engineering Consultants, LLC.

As mobility tools change the way we live, so do they impact how healthcare delivers its services. From care providers to patients, totally new ways are opening for accessing healthcare services, for gaining treatment and for managing disease conditions like never before.

Patients can ask their care provider questions from anywhere while using mobility tools such as a laptop, tablet and smart phone. Healthcare professionals, at the same time, are able to extend their desk workstation to follow them as they travel, thus enabling immediate response to changes in their patient's conditions. They also are able to participate in more skills-development and education activities not limited by time and location, as these opportunities are also available anywhere they are.

Mobility tools are welcome facilitators to a better healthcare delivery system.
The tasks assigned to these tools vary in scope and criticality. In July 2007, doctors successfully implanted a sophisticated pacemaker and defibrillator in former VP Dick Cheney's chest, thus saving his life. The implanted defibrillator senses when the heart's electrical activity has misfired and induces a quick zap to jolt the heart back into a normal, healthy beat. The implanted defibrillator communicates with the cardiologist's workstation when changes need to be made to its function or when review of heart rhythm history is needed. Some mobility tools, like the implanted defibrillator and smart infusion pump, are life-support devices, while others are used as diagnostic tools or communication devices, such as the iPad tablet. These tools contain embedded intelligence and communication. They are able to store personal information that must be protected, and the access to it must be well managed as well.

The transition within healthcare, from physical paper-based files of health records piled up in the medical records storage rooms to the electronic repository of paperless medical records (EMRs), is a major change that must be progressed along a secure plan that protects the information contained in it.

Together with the remarkable benefits that the mobility tools offer, the communication between the EMR and the rest of the system, including the medical devices, is a new challenge that must be managed to make these applications safe, effective and secure.

These healthcare systems of networks that contain mobility devices, medical devices and depositories like EMRs are special in two important respects.

First, they store and transmit data that is uniquely sensitive, and therefore governed by rigorous, industry-specific privacy regulations like the U.S. Health Insurance Portability and Accountability Act (HIPAA). Second, network-connected healthcare devices expose healthcare networks to a broader range of security and privacy risks than the "typical" wired network of desktops and laptops.

The recently approved (November 2010) international standard IEC 80001-1 for the "Application of Risk Management for IT-Networks Incorporating Medical Devices" describes the application of a risk-management process into the design, deployment and on-going management of an IT network connected to a medical device and is essential for the creation of a safe, secure and effective network used by healthcare delivery organisations and their partners.

Additionally, the accompanying technical report draft titled "Part 80001-2-x: Guidance for Wireless Networks" applies the same concept of risk-management roles, responsibilities and activities necessary for the maintenance of confidentiality and the protection from malicious intrusion that otherwise might lead to compromises in the integrity of the system or in the availability of authentic data. The need for this risk-management programme derived from the rise in the volume, sophistication and focus of malware, raising the likelihood of, and damage from, malware attacks and data breaches, according to a September 2010 survey by the College of Health Information Management Executives (CHIME) called "Networked Medical Devices—Security and Privacy Threats: Healthcare IT at a Crossroads."

In addition, according to the Wi-Fi Alliance manuscript "Wi-Fi in Healthcare: The Solution for Growing Hospital Communication Needs" (February 2011), more than 5,00,000 Wi-Fi infrastructure end-points were deployed in U.S. healthcare facilities in 2010, representing a 50 per cent increase from 2009. Worldwide sales of Wi-Fi technology into the healthcare market are expected to reach $4.9 billion [Rs.21,973.09 crore] in 2014. This growth trend of use and of threats places the IEC-80001 standard in a critical position that offers both the needed methodology and the governance structure for safety and security of hospitals' systems that incorporate these mobility tools. The features outlined in the standard include a set of controls that are intended to increase the protection of both data and systems with special attention given to the protection of personal and its subset health-related data.

The IEC-80001 standard together with the proposed technical reports identify structure and processes that can be implemented by responsible organisations and their vendors as supplemental to their existing or new end-to-end safe and secure network risk-management programme. This will allow for medical device mobility and security to co-exist.

- **Yadin David**
IEEE Senior Member