The Promise and Peril Of Wireless Technologies

Rick Hampton, Steve Baker, and Ken Fuchs

There is no denying the fact: Wireless, in all its forms, is hot. We’re deluged with news of how new wireless technologies will change the face of healthcare. They will lower costs, increase quality, make up for the coming shortage of doctors and nurses, connect the most rural of hospitals and clinics, move healthcare to the home, eliminate alert fatigue … indeed, the list seems endless. There is little question that such functionalities are desperately needed and that wireless makes many of them possible. It comes about because of the relative ubiquity and ease of developing applications for consumer wireless devices.

As much as these new wireless technologies are a blessing, they can also be a curse. While anyone can now connect virtually anything to everything else, it’s often left up to the end user to determine whether the application and infrastructure is fit for the purpose and use. The end user becomes a critical participant in the development of the device and application, a role that most have never before performed.

To grasp the solutions enabled by wireless technologies and avoid their foibles, we must better understand their strengths and weaknesses. The articles in this section discuss the key topics important to implementing good risk management practices while integrating medical devices with IT networks using wireless technologies.

First, with any new technology there comes a new vocabulary and jargon. To help the reader keep up to date, we’ve included a glossary.

Then, Don Witters provides a unique perspective of the uses and development of wireless technologies within the medical devices themselves while presenting the risks and challenges of wireless medical networks. Much of his discussion was used earlier in developing the U.S. Food and Drug Administration’s Draft Guidance for Industry and FDA Staff: Radio-Frequency Wireless Technology in Medical Devices (2007). Be sure to include this document on your “must-read” list. You’ll have a better understanding of the risks medical device manufacturers must address in their product development efforts.

Next, Phil Raymond and Rick Hampton discuss the application of risk management to wireless medical networks. It is the essence of the draft IEC 80001-2-3 Wireless Guidance Technical Report to which we all contributed. While most people think of wireless medical networks as consisting only of hospital Wi-Fi networks, we address other systems as well.

Finally, Jim Moon discusses the “Holy Grail” of the problem that began with the first electronic medical device—management and verification of clinical data (e.g. alarms) on a wireless medical network. The FDA’s Manufacturer and User Facility Device Experience (MAUDE) database contains many examples of past and present systems that have resulted in patient compromise and death because they omitted one or more points presented here. With alarm management the hot topic it is today, everyone should find this article informative.

Steve Baker and Ken Fuchs compiled problems reported to us into short case studies, sprinkled throughout the section. Here you will find object lessons in good intentions vs. the law of unintended consequences. No, they aren’t made up. They really happened. Names have been removed to protect the embarrassed. These examples should give us all pause about whether our risk management activities are as sufficient as we would like to believe.

We hope you find these texts clear and compelling examples of why your healthcare institution should begin addressing risk management of these increasingly integrated and complex systems of medical devices and IT networks.

About the Authors

Rick Hampton is the wireless manager for Partners Healthcare System. E-mail: rhampton@partners.org

Steve Baker is a principal engineer at Welch Allyn Monitoring. E-mail: steve.baker@welchallyn.com.

Ken Fuchs is a senior principal architect for enterprise systems at Mindray North America. E-mail: k.fuchs@mindray.com