Abstract — Electromagnetic compatibility (EMC) is a critical part of addressing the risks related to the effects of electromagnetic interference (EMI) on active medical devices exposed to emissions from wireless technology. In addition, for wireless technology in healthcare to be safe, effective, reliable, and secure specific wireless issues must also be addressed including quality of service, coexistence with other wireless equipment, data integrity, and wireless security. Unfortunately, these issues pose risks that are poorly addressed in present medical devices standards or other consensus documents. This paper discusses risks for wireless technology in healthcare with examples from research examining the effects of emissions from wireless technology such as RFID on implantable cardiac pacemakers and defibrillators and EMC with other emitters. The paper goes into ways that the risks, including EMI, can be addressed and makes the case for substantive engagement by stakeholders, including the IT community, wireless developers, and clinical organizations. There is clear need to develop unbiased, consensus information and tools that will set the pathways and tools needed to meet the risks and challenges for widespread incorporation of wireless technology in healthcare.

I. EMC AND WIRELESS TECHNOLOGY IN HEALTHCARE

The risks of electromagnetic interference (EMI) to active medical devices is well recognized [1,2] and partially addressed through appropriate design and testing to consensus standards such as IEC 60601-1-2 [3] for medical electrical equipment, ISO 14708-1 [4] for active implantable medical devices, and ANSI/AAMI PC69 [5] for implantable cardiac pacemakers and implantable cardioverter defibrillators. However, these standards concentrate on EMC aspects of the medical device and its function and pay minimal attention to the incorporation of wireless technology. In addition, these standards do not adequately touch upon issues associated with the deployment of wireless technology [6, 7]. The IEC 60601-1-2 standard contains allowances that exempt certain testing of the wireless technology incorporated into the medical device under test because the radiated immunity testing is expected to disrupt the wireless data transmission using the same RF frequency band. Further, these standards address generalized environmental electromagnetic (EMI) emitters and exposures without regard to certain RF wireless emitters that have been linked to medical device EMI such as radiofrequency identification (RFID), anti-theft and security systems and cellular (mobile) telephones.

Concurrently, wireless technologies such as IEEE 802.11 and Bluetooth are being incorporated into medical devices like surgical control devices, infusion pumps, patient monitoring devices, and blood glucose monitors. Coexistence of the medical device wireless technology with other wireless products or systems including other devices operating in the vicinity is a concern and may present additional potential risk such as the disruption the medical function.

Risk for EMI is also related to the medical device function and how critical this may be for the patient safety and device effectiveness. We performed a survey of medical device experts and clinicians within FDA that revealed high priority concerns from EMI over a wide range of medical devices that are summarized in table 1.

<table>
<thead>
<tr>
<th>Type of device</th>
<th>History of EMI</th>
<th>Potential consequence of EMI disruptions</th>
<th>Major Category of use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardiac pacemaker, implantable defibrillators</td>
<td>High</td>
<td>High</td>
<td>Life supporting</td>
</tr>
<tr>
<td>Drug infusion pumps</td>
<td>High</td>
<td>High</td>
<td>Life supporting</td>
</tr>
<tr>
<td>Wireless telemetry monitor devices</td>
<td>High</td>
<td>High</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Implantable deep-brain stimulators</td>
<td>Moderate</td>
<td>High</td>
<td>Therapeutic</td>
</tr>
<tr>
<td>Infant incubator-warming devices</td>
<td>High</td>
<td>High</td>
<td>Life supporting/therapeutic</td>
</tr>
<tr>
<td>Wireless medical data entry computers</td>
<td>High</td>
<td>High</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Ultrasound therapeutic devices</td>
<td>Moderate</td>
<td>High</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Powered wheelchair/scooter devices</td>
<td>High</td>
<td>Moderate</td>
<td>Transport</td>
</tr>
<tr>
<td>Wired medical data entry computers</td>
<td>High</td>
<td>High</td>
<td>Diagnostic</td>
</tr>
<tr>
<td>Active ventilators-respirators</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Life supporting</td>
</tr>
<tr>
<td>Anesthesia devices</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Therapeutic</td>
</tr>
<tr>
<td>Hemodialysis medical devices</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Life supporting</td>
</tr>
</tbody>
</table>
In addition to EMC, there are risks for patient safety inherent in medical uses of wireless technology particularly where the wireless technology carries alarms, is integral to the medical function such as closed loop, or provides remote control functions. These risks relate the function and intended use of the medical device with the security, temporal and quality needs for the data as even momentary loss or degradation of healthcare wireless signals can manifest in serious patient harm.

The emissions from wireless technology can be a source of potential interference and at the same time it can be a victim of EMI, cross-talk, or other communications problems. In addition, medical device systems using wireless technology can be vulnerable to newer technology and changes in the spectrum use such as occurred to wireless medical telemetry resulting from changes to the Private Land Mobile Radio Service. [8] Moreover, unlike other uses of wireless technology the world of medical devices are constrained by the characteristics of the human body and the functions performed. For example, implanted cardiac pacemakers and cardioverter defibrillators (ICDs) must operate with sensitivity to the naturally occurring electrical activity of the heart ranging from dc to several kHz and higher, modulated by the heart beat frequency (Figure 1). These devices must sense signals with characteristics in the areas lying above the curves (pacemaker sensing curve and ICD sensing curve, respectively). The devices are designed to recognize and reject signals below the respective curves.

Figure 1  Sensing thresholds for implantable cardiac pacemakers and implantable cardioverter defibrillators (ICD). (Figure courtesy of Medtronic)

In recent years the deployment of RFID into health care has accelerated to provide mobility for such tasks as connecting and tracking medical equipment, medicines, blood products, and in some cases patients and clinicians. The increased penetration of cellular telephone technology has allowed communications among clinicians, caregivers and patients. However, there are demonstrated EMI effects on medical devices if cellular telephones are allowed in proximity to susceptible active medical devices. [9-11] Wireless security systems such as metal detectors and anti-theft systems have also affected medical devices. [12]

A. RFID EMI effects on implantable medical devices

In the U.S. RFID works primarily in three RF frequency bands: 134 kHz, 13.56 MHz, and 915 MHz. Recent studies in Europe and the U.S. have demonstrated that a range of active medical devices can be susceptible to EMI from the emissions of certain RFID products. Van der Togt et.al. [13] showed that up to 63% of the medical device tested could manifest effects when exposed to certain RFID technologies. Seidman et. al. [14] observed that 83% of the implantable cardiac pacemakers tested showed effects to 134 kHz RFID, 18% to 13.56 MHz, and 6% to 915 MHz. A more recent study indicates similar results [15].

B. EMI effects at 915 MHz

Significant effects of EMI were observed in several high priority medical devices exposed to a proprietary signal centered in the 915 MHz ISM frequency band. Figure 2 shows the malfunction and alarm induced by RF exposure to a syringe pump device used to infuse measured doses of drug during such critical therapies such as chemotherapy for cancer treatment. This type of effect was rated as potentially high risk for patient safety by physicians who emphasized the potential harm that could be caused by the disruption of critical therapy.

Figure 2 Malfunction observed in syringe infusion pump medical device after exposure at 915 MHz that could result in significant medication dispensing error.

Other devices tested including an automatic external defibrillator and critical-care ventilator. Significant effects caused by the RF exposure were observed.
C. Wireless technology coexistence

While there are several consensus standards focusing on EMC for medical devices [3-5], the issues involving wireless technology are not so well addressed. For example, coexistence among RF wireless technologies can be an issue and present a risk in the healthcare setting depending upon the intended use of the wireless technologies. Sakal and Simunic [16] showed the probability of interference among common wireless communications technology such as Bluetooth and IEEE 802.11 can be significant particularly as more emitters are collocated. Golmie et.al. [17], among others, note the challenges for coexistence among in-band wireless technologies. Our study of coexistence among Bluetooth and IEEE 802.11 technologies confirmed that significant disruption of the data traffic can occur and can increase as the number of wireless emitters increase.

III. ADDRESSING EMC AND WIRELESS RISKS

Wireless technology can be beneficial to the delivery of medical care particularly in the transmission of patient physiological and treatment information. However, there are risks that can result in patient harm either directly during diagnosis or treatment or indirectly such as loss of or degradation of patient information. The range of risks vary from lower risks associated with non-vital or historical information where loss or delay have little affect on the patient, to medium risk for such tasks as the transmission of diagnostic information that can withstand degradation (e.g., corruption in cardiac signals for a non-critical patient where the corruption is easily recognized by a trained clinician), to high risk functions like remote control of vital therapy such as infusion of drugs or blood products where even momentary lapses in a wireless signal can have serious consequences.

Recognition of the uses and risks associated with wireless technology in healthcare is key to conceiving, designing, testing, and maintaining safe, secure and reliable healthcare systems that include wireless technology. Among the issues that must be addressed are:

- quality of service that is known and achievable
- coexistence with present and foreseeable future wireless technology inside and outside the facility
- data integrity, including reliable, consistent data latency and throughput
- wireless security adequate for the use and medical function
- EMC of the wireless technology and the medical devices used in the vicinity

These issues and how they should be addressed for wireless medical devices are discussed in the FDA document Draft Guidance for Industry and FDA Staff Radio-Frequency Wireless Technology in Medical Devices [18].

V. CONCLUSIONS AND CHALLENGES

The use of wireless technology in healthcare presents great promise and challenges. Among these are risks beyond EMC that go to the heart of the ability for proper medical device and system function in an increasingly harsh electromagnetic environment crowded with more and more wireless technology components performing an increasing number of tasks. While there are standards for medical device and system EMC these are inadequate to address the flow of vital patient data and medical device control via wireless technology. There is great need for the creation of processes, protocols, design and deployment guides, standards and educational tools geared to the unique needs of healthcare. This is especially needed now as the trend is toward shorter stays in medical facilities and incentives to provide more care at home where medical expertise and oversight are much less available. Stakeholders including the medical device industry, the IT and wireless industries, and the healthcare community must come together now to develop cohesive strategies, information and tools for the safe, effective, secure and reliable use of wireless technology in healthcare.

ACKNOWLEDGMENT

The authors wish to acknowledge Christina Ortega, Bonnie Markovitz, and F.K. Umberger for their contributions in the survey and laboratory efforts used in preparing this paper.

REFERENCES


