

Wireless and Mobile Technologies for Healthcare: Ensuring Privacy, Security, and Availability

T. Jepsen, N. Buckley, D. Witters, K. Stine

INTRODUCTION

The IEEE-USA Medical Technology Policy Committee sponsored a session on some of the privacy, security, and reliability concerns for healthcare IT, and specifically in using wireless technology for the transmission of healthcare-related information, as part of the First AMA-IEEE Medical Technology Conference on Individualized Healthcare, held March 21-23 at the Renaissance Mayflower Hotel in Washington, DC. Examples of healthcare IT using wireless technology include:

- The use of handheld devices to record medical information
- Medical instrumentation
- Home healthcare functions
- Use of wireless by emergency responders
- Broadcast of healthcare alerts via public networks.

The panel discussion took place on Monday, March 22, from 1:00 – 2:15 pm. The program consisted of presentations by experts from healthcare providers and government agencies. The goal of the session was to define actions where IEEE resources such as standards development can partner with other standards groups, government agencies, clinicians, and healthcare organizations to develop safe, reliable, and secure wireless healthcare technology.

Presentations addressed the following topics:

- An overview of privacy and security concerns for healthcare IT
- A survey of different wireless technology used in healthcare now, including traditional wireless medical telemetry, WiFi, RFID and emergency radio systems
- The risks and mitigations for wireless healthcare and the underlining issues, to include examples of how things really work in the clinic
- Privacy and security requirements for certification of EHRs under Meaningful Use criteria.

Presentations and presenters were:

- “Managing Wireless Medical Device Security Challenges in Today’s Enterprise Healthcare.” Neil W. Buckley, Enterprise Information Security Architect, Partners Healthcare System (nwbuckley@partners.org)
- “Building Pathways to Safe, Secure, and Reliable Wireless Healthcare.” Donald M. Witters, Office of Science and Engineering Laboratories, Center for Devices and Radiological Health, Food and Drug Administration (donald.witters@fda.hhs.gov)
- “NIST’s Role in Securing Health Information.” Kevin Stine, Information Security Specialist, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology (kevin.stine@nist.gov)

Each presentation is summarized separately below.

PRESENTATION SUMMARIES

“Managing Wireless Medical Device Security Challenges in Today’s Enterprise Healthcare,” Neil W. Buckley

Neil Buckley began with an overview of Partners Healthcare organization and operations. Partners Healthcare is a non-profit organization founded in 1994 by Brigham and Women’s Hospital and Massachusetts General Hospital. It provides both primary and specialty care at 11 hospitals and 140 care locations. It employs 6300 physicians and has annual revenues of \$7.9B.

Buckley then described wireless infrastructure for HIT. Wireless access points are provided to enable wireless access to client devices as part of the overall enterprise architecture. Multiple wireless protocols are employed in the network, including WiFi with Bluetooth. Authentication schemes are complex due to the need to support a wide variety of protocols and user applications.

Another factor to consider is the building environment. Often the wireless infrastructure must operate in buildings with a variety of construction techniques. Shielding may be present in some environments, and may impede wireless connectivity.

Stakeholders who may influence the architecture of the wireless infrastructure include

- Clinicians
- Business Owners
- Medical Device/Software Manufacturers
- Federal/Local Governments
- Internal/External Auditors
- Information Technology Industry
- Information Technology Team

Some of the security challenges presented by wireless include the rapid evolution of markets and standards and the need for automation. Risk mitigation strategy needs to be balanced against tactical concerns. Enterprise systems architects need to create a technology acquisition model.

Architecture and design of the wireless infrastructure must be based upon user requirements. In most cases, this is the clinician. Important requirements include

- Low risk (do no harm)
- Extensive mobility
- Ease of use
- Universal access
- Fast
- Available
- Reliable

Technology requirements create challenges for medical technology manufacturers. Enterprise integration capabilities are typically limited, and solution requirements differ drastically. Information technology manufacturers must deal with solution requirements that change rapidly, and must provide solutions for common devices.

Information technology teams will typically develop requirements for service level agreements (SLA). Their requirements will also be based on a chosen platform.

Governance covers a wide spectrum of regulatory requirements and rules. Governance requirements come from a wide variety of government, accreditation, and standards organizations, including

- HIPAA
- ARRA HITECH Act
- FDA
- FAA
- JCAHO
- NIH
- Federal and State Law
- PCI DSS
- Record Retention
- GLP 21CFR58
- Meaningful Use
- Standards Organizations, including NIST, ISO, ITIL, and ATNA

Buckley presented a use case involving wireless technology for administration of medications using “smart pump” technology. This application would have the ability to improve patient safety and clinical workflow. It would have impact in the areas of 802.11 infrastructure, clinical platform risk factor, and support roles and responsibilities.

However, use of this technology would create a requirement to better identify the individual patient receiving the therapy via wireless. This might be an area where licensing of a wireless application might be an option.

In conclusion, Buckley presented some thoughts on the future of healthcare information technology. Some future challenges include

- Infrastructure must be reasonably priced, portable, and leverage existing support models
- Infrastructure must be reliable, scalable, safe, and secure
- Existing governance bodies must be consolidated
- Assistance must be ubiquitous and incentives must be aligned.

“Building Pathways to Safe, Secure, and Reliable Wireless Healthcare.” Donald M. Witters

Donald Witters’ presentation began with a graphic of a test showing electromagnetic interference (EMI) created by a Blackberry handheld device exposing a cardiac ultrasound device. He gave an overview of wireless applications for healthcare which are being integrated into all healthcare environments, including

- Home
- Hospital
- Transport
- Rescue
- Nursing Homes
- Doctor’s Offices
- EHR
- Military

This rapid integration creates challenges for wireless technologies. A major issue is EMI because a radiofrequency (RF) wireless application may be a source of interference for another application, or it may itself be disrupted by EMI. Multiple wireless transmitters must coexist in the same environment. Interoperability and network convergence are also important considerations. Security for wireless medical devices and systems needs to be addressed; also needed is a clear definition of “good enough” security for the risks involved. However, existing standards, including the IEEE 802.11b wireless standard, are inadequate to address these issues. A clear definition of what is required for “medical grade” wireless is also needed.

Some of the issues that need to be addressed for wireless medical systems include

- Risk –currently being addressed in the IEC 80001 standard under development
- Security – what are the risks and what is “good enough?”
- Manageability, including expandability, changeability, upgradeability

- Availability
- Resilience
- Quality of Service
- Integrity
- Coexistence
- Certification
- Privacy and Confidentiality
- Information provided in the labeling such as user manuals

Witters presented an overview of the frequency allocations in the 2450 ISM band allocated to medical applications. Many of the subchannels allocated to 802.11b/g and 802.15.1/3/4 overlap, thus creating an opportunity for interference. Common devices such as microwave ovens, cellphones, laptop computers, and handheld devices may also be sources of interference. Coexistence testing in a controlled environment enables potential interference to be identified and characterized.

There are specific concerns about medical system security in addition to the basic requirements for patient information provided by the HIPAAA Final Security Rule. The security concerns can be specific to wireless applications and include

- Authentication – ensuring authorized users
- Encryption – for the wireless links to secure sensitive data
- Open Architecture – that were not designed specifically for medical applications
- Multiple combinations of technologies
- Rogue wireless users

Existing technologies for wireless security include Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA). WEP is not considered to offer adequate security. WPA and the more recent WPA2 provide stronger encryption security.

Witters identified the following needs for medical wireless:

- Clear pathways for safe, secure and reliable deployment, use, and maintenance
- Framework and consensus standards for wireless technology in healthcare —to include shared risk management, definitions, consistent test methods, certification and deployment information
- “Medical Grade” wireless – definition, characterization, risk management
- Stakeholder communication and engagement—stakeholders need to be identified, including clinicians, users, healthcare organizations, manufacturers, vendors, IT, standards organizations, VA, DoD, businesses.

In summary, wireless healthcare holds much promise and many challenges. There is a lack of adequate tools and clear pathways for safe, secure and reliable wireless healthcare. Standards and other information are needed, including frameworks, test methods, and a definition of “medical grade” wireless. IEEE needs to take on a

leadership role, along with other stakeholders to develop goals, pathways, and consensus standards. Making wireless healthcare work requires research, risk awareness and management, stakeholder engagement, and a proactive approach to safe, secure, reliable deployment.

“NIST’s Role in Securing Health Information,” Kevin Stine

Kevin Stine’s presentation began with an overview of NIST’s mission, which is “to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.”

The mission of the Computer Security Division is to provide standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services, in order to build trust and confidence in information technology (IT) systems.

Stine then discussed NIST’s role in developing the conformance test methods (test procedures, test data, and test tools) to ensure compliance with the meaningful use technical requirements and standards. As defined in the Notice of Proposed Rulemaking (NPRM) on the definition of “meaningful use,” professionals and hospitals eligible to receive payments under the Medicare and Medicaid EHR incentive programs must be able to demonstrate meaningful use of a certified EHR system.

The proposed standards and certification criteria, identified in the Standards and Certification Interim Final Rule (IFR), are linked to and specifically designed to support the 2011 meaningful use criteria. For Stage 1, beginning in 2011, adequate privacy and security protections must be ensured for personal health information.

Stine then gave an overview of NIST’s past, present, and future security activities. Risk Management consists of six steps, each with associated documentation in the form of Federal Information Processing Standards (FIPS) and Special Publications (SP). Starting with organizational input, this process leads to development of an architecture description for security.

NIST’s involvement with health IT security has focused on three areas:

- Standards Harmonization – support of ONC and HITSP in harmonizing and integrating standards to enable exchange of health information
- Outreach and Awareness – present on application of security standards and guidelines to HIPAA and HIT security implementations
- Publications and Resources – HIPAA Security Rule Guide, HIE Security Architecture

In the future, NIST will address the following areas:

- Security Automation – HIPAA Security Rule Toolkit, Security Configuration Checklists
- HIT Test Infrastructure – Provide capability for current and future EHR testing needs against standards, conformance and interoperability testing capabilities

NIST has developed a set of recommendations for implementation of secure wireless and mobile technologies:

- **Wireless**
 - 800-127 Draft, Guide to Security for WiMAX Technologies
 - 800-121, Guide to Bluetooth Security
 - 800-120, Recommendations for EAP Methods Used in Wireless Network Access Authentication
 - 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
 - 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks
- **Mobile Technologies**
 - 800-124, Guidelines on Cell Phone and PDA Security
 - 800-114, User's Guide to Securing External Devices for Telework and Remote Access
 - 800-101, Guidelines on Cell Phone Forensics
 - 800-46 Rev 1, Guide to Enterprise Telework and Remote Access Security

PANEL SUMMARY

The panelists presented a diversity of viewpoints on the need for effective standards and test methodologies to ensure that wireless applications for healthcare provide adequate privacy, security, and reliability.

After the panelists had presented, the panelists answered questions from the audience. Audience members mentioned the need for authentication for the Nationwide Health Information Network (NHIN), the use of biometric technologies for authentication, and security for wireless healthcare applications as part of the FCC National Broadband Plan.

Recommendations for Going Forward

Panel members were asked to identify the highest priority steps needed to go forward with ensuring privacy and security for healthcare wireless applications. The panelists recommended the following:

- Creating consensus among stakeholders and standards organizations regarding the need for wireless security, privacy, and reliability standards

- Development of effective standards and related documentation (e.g. testing standards)
- Development of reference architectures for wireless security in enterprise environments
- Use of an “open process” for standards development.

On behalf of IEEE-USA, I would like to thank the panelists for their valuable contributions to the effort to make secure, private, and reliable medical wireless a reality.

Thomas C. Jepsen
Chair, IEEE-USA Medical Technology Policy Committee
tjepsen@ieee.org
March 31, 2010