'This Process Is Just Beginning' Connecting Mobile Medical Devices

Terenzio Facchinetti, Anura Fernando, and Richelieu Quoi

Historically, medical devices have been (and to a large extent still are) built as stand-alone devices, and when they were integrated into a system, a closed-loop topology (i.e. one providing regulation through a feedback control mechanism) ensured greater control. Today, medical devices are evolving to reap the advantages of wireless connectivity, primarily by adopting proprietary system architectures based on off-the-shelf components.

The development and rapid evolution of wireless communication makes it possible for patients and clinicians to communicate easily, thus enabling efficient information transfer through a broad spectrum of technological infrastructures, from silicon microelectronics to networked systems of systems.

A technological progression from second generation to fourth generation mobile communications is currently taking place, with the added advantages of increased versatility, robustness, and ability to keep pace with the rapid evolution of processing capabilities, i.e. dynamic adaptation to mobile platforms.

As a result of this emerging technology, medical and many other devices are becoming increasingly interconnected and will, in the future, be fully interoperable. However, this process is just beginning, and a fully mature, interconnected, and viable medical device ecosystem has yet to be established.

For the successful development of this type of ecosystem, device and network safety must be ensured. In standards such as ISO 14971, *Medical devices—application of risk management to medical devices,* the term 'safety' is universally understood to mean freedom from unacceptable risk. There is increasing concern in the fields of eHealth (electronic health) and mHealth (mobile health) about unintended consequences or "risks" to patients, users, and/or the environment which could result from integrating medical devices and IT technologies.

Mobile technology is improving in leaps and bounds—but who is eavesdropping?

If safety is not established, patients and providers will reap far fewer benefits from eHealth and mHealth technologies than would otherwise be the case. To ensure security, a number of constituents not unique to mobile-communication—such as stand-alone medical devices (legacy products), embedded software, apps, mobile platforms, architecture, and infrastructure—will have to be evaluated.

Each eHealth and mHealth constituent should be able to operate both unconnected and/or within the context of a safe system

About the Authors

Terenzio Facchinetti, PhD, is UL's Life & Health business development manager. He has also managed pharmaceutical research, international medical devices, and in vitro diagnostics. E-mail: terenzio.facchinetti@ul.com

Anura Fernando is UL's principal engineer for eHealth—medical systems interoperability and mobile health. E-mail: anura.s.fernando@ul.com

Richelieu Quoi is UL's specific absorption rate (SAR) technology consultant, and a reviewer for the U.S. Federal Communications Commission (FCC) SAR telecommunication certification body (TCB). E-mail: richelieu.quoi@rfi-global.com

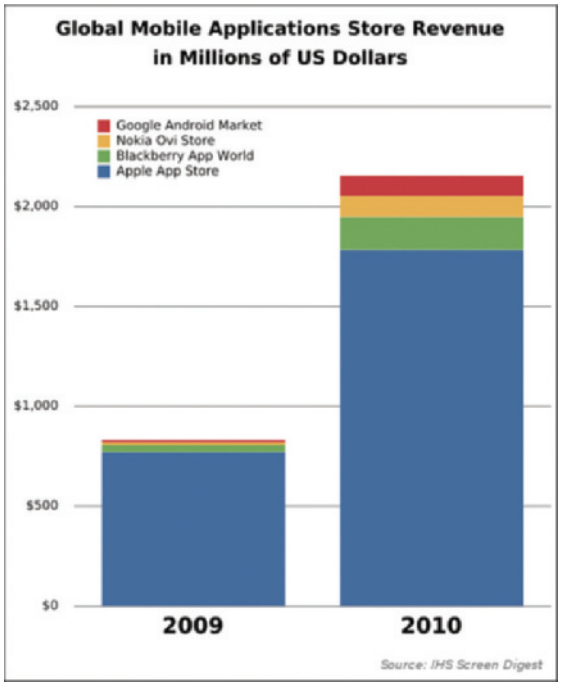

Figure 1. Growth of mHealth App Market According to Mobile Platform Type

framework. In this article, we present an overview of mHealth system technology, and highlight areas that should be evaluated from a safety perspective when connecting mobile health devices.

Defining mHealth Within the Context of eHealth

mHealth refers to the use of mobile devices such as smartphones, tablet computers, personal digital assistants (PDAs) and other such platforms; as well as computer software applications (apps) in support of healthcare delivery within hospitals and outside their physical walls. The tremendous increase in the use of healthcare apps, particularly those available for Mac/iPhone/iPad users is notable (Figure 1).

As demand for mHealth devices and services has increased, mHealth has become more narrowly defined. In 2005, mHealth referred to "emerging mobile communications and network technologies for healthcare."[1] At the 2009 mHealth Summit of the Foundation for the National Institute of Health (FNIH), mHealth was defined as "the delivery of healthcare services via mobile-communication devices."[2]

eHealth, a much broader category that encompasses mHealth, is defined by the World Health Organization (WHO) as a "cost-effective and secure use of information and communications in support of health and health-related fields, including healthcare services, health surveillance, health literature, as well as health education, knowledge, and research."[3]

Globally, governments strive to improve healthcare through eHealth, aiming to:

- Improve the quality of and access to healthcare
- Contain exploding healthcare costs
- Stimulate growth in the medical industry

Advances in eHealth are expected to lead to significant improvements in healthcare through, for example, telemedicine, teleHealth, telecare, electronic health records (EHR), electronic medical records (EMR), medical device interoperability, and other health information technologies.[4,5]

The safe development and use of healthcare information technologies and interoperable medical devices may reduce a variety of common systemic problems such as prescription errors, adverse events related to drug delivery and clinical decision support, and harm or death related to manual errors and inadequate closed-loop feedback.

eHealth also has the potential to reduce time of hospitalization (by improving speed and accuracy of clinical decision support with related treatment) and facilitate more targeted patient treatment (such as remote monitoring of elderly patients at home), thus reducing the extent of exploratory or broad-spectrum acute and chronic treatments, as well as their associated healthcare costs.

To achieve longterm healthcare objectives, the industry and its regulators will need to explore and implement new technologies and approaches, possibly sharing and merging competences that have been, until now, primarily associated with other commercial sectors, such as information technology (IT) and telecommunications.

The mHealth Ecosystem

Various new industry players are helping to shape a new healthcare ecosystem with the potential to deliver the benefits outlined and develop innovative new technologies. Information and communication technology (ICT) manufacturers and service providers such as smart phone manufacturers, operators,

telecommunications infrastructure providers, app developers, educators, users, and traditional medical device manufacturers are all pushing technological boundaries and exploring new possibilities heretofore not even considered to be within the realm of healthcare.[6]

This change is expected to help drive a dramatic expansion of the mobile device market, with an estimated 18.0% compound annual growth rate (CAGR) between 2010 and 2016, and 4.9 million remote-monitoring connections expected by the end of 2016.

While it may appear that mHealth is primarily applicable to remote healthcare and caregivers using consumer cellular communication infrastructure, current trends indicate that it may be equally utilized within local area networks or LANs (such as hospital IT infrastructure), body area networks or MBANs (for monitoring individuals' physiological parameters), and similarly localized network infrastructure. The recent U.S. Federal Communication Commission (FCC) allocation of spectrum for MBANs also supports further use in this area.

mHealth may ultimately lead to a scenario where the physician, other clinician, or caregiver will request not only patient records, but also diagnostic results, real-time patient monitoring data, and other essential data via mobile media, as soon as the data becomes available (and potentially for real-time diagnosis and treatment). Mobile health is likely to play a significant role in the large application sectors of telemedicine and remote healthcare, especially in isolated communities with low population densities, developing countries, or in other resource-poor environments.[6,7]

Impact of mHealth

The UN Millennium Development Goals (MDGs) are still far from being reached.[7] In 2008, children in developing countries were 33 times more likely than children in the developed world to die from diseases that could be prevented by basic medical services and vaccination. Women were still dying at the rate of one per minute due to complications during pregnancy and childbirth, and an estimated 2.5 million new HIV infections occurred in 2007, compounded by a shortfall of healthcare workers in 57 countries, most developing.[6]

mHealth may alleviate these and other public health and safety issues by:

- Providing access to remote data collection and monitoring disease and epidemic control
- Increasing the number of successful treatments and interventions
- Improving diagnostics and treatment support
- Facilitating a healthy lifestyle
- Improving decision making by health professionals and patients
- Increasing awareness of medical and health information in the general population
- Enhancing healthcare quality via improved access to patient data and healthcare information
- Facilitating the training of healthcare providers and workers

A number of mHealth projects are designed to support healthcare workers in remote areas in the diagnosis and treatment of patients. Some provide advice and step-by-step medical decision support, while others provide a direct diagnosis. Education and training projects can connect healthcare workers to remote sources of information, other staff, institutions, and/or experts via mobile phones.

Mobile health is likely to play a significant role in the large application sectors of telemedicine and remote healthcare, especially in isolated communities with low population densities, developing countries, or in other resource-poor environments.

Mobility-based and cloud-based services linked to advanced medical technologies will have a big impact on the future of healthcare, including the challenges currently being faced in the US. For example, in 2011, diabetes was associated with 40% of healthcare spending. By 2020, it is projected that 12% of the U.S. GDP may be associated with expenditures related to diabetes and other chronic diseases.[7]

Public and industry awareness of mHealth is growing, although a new June 2012 study for PricewaterhouseCoopers, "Emerging mHealth: Paths for Growth," suggests that consumers are more ready than industry to adopt mobile health.[8] According to the press report, mHealth in developing countries is a means to get increased access to healthcare, whereas in developed countries it is a "way to improve the convenience, cost and quality of healthcare."

Mobile Technologies: Infrastructure and Penetration

Technological infrastructures such as cellular communication may make it possible to bridge the global mHealth gap. Cellular

infrastructure facilitates both circuit-switched transmission—a dedicated and exclusive route for voice usage—and packet switched transmission, with no pre-determined route (typically for data usage).

As data usage soars to new heights, cellular technologies have begun to improve their data throughput and latency with increased technology bandwidth and frequency spectrum, made possible by third generation (3G) and long term evolution (LTE), or fourth generation (4G) technologies. Mobile usability for internet-based applications is becoming as prolific as home broadband service. The deployment of LTE technology will allow many establishments to fully utilize mHealth.

3G is one of the strong points of cellular technology, supporting higher data throughput and boasting an ongoing evolution such as evolved high-speed packet access (HSPA+). Second generation (2G) networks are also well established and cost-efficient, making global packet radio service/enhanced data for global evolution (GPRS/EDGE) services such as short message service (SMS or texting) services accessible almost anywhere in the world.

Although GPRS/EDGE services have slower data rates than 3G or 4G services such as multimedia messaging services (MMS) and voice over internet protocol (VoIP) services, they can allow users in developing countries with this infrastructure in place to access healthcare information.

Cellular technology used for mHealth will, in the future, be expected to function in real time, so data latency—the time taken to collect and store the data—must be addressed from a security perspective.

Smartphones and tablet PCs, an integral part of and a gateway to cellular networks and servers, are at the forefront of mHealth due to their popularity, size, and vast functionality. These 'magic box' platforms support multiple wireless technologies, and in some instances, are part of a medical ecosystem that integrates a closed-loop system, such as a noninvasive blood pressure monitor (NIBP), or an open-loop system supporting patient monitoring devices.

However, smartphones and tablet PCs have security limitations: Device content can be cloned, and/or the information extracted much more easily than in other hardware, given their size, the fact that they are carried everywhere, and are used to store personal and private information. Medical apps can be targeted by malware. Other mobile devices (in one specific instance, a wireless insulin pump) have been shown to be just as easily 'hacked,' allowing device functions to be tampered with.

Therefore, in addition to impacting privacy, this lack of security can impact safety ('safety' and 'security' not being interchangeable concepts), leading to patient harm, for example, if a patient's data or mobile device function is altered. Although it may never be possible to have completely secure mHealth, there is a good chance that by targeting possible security risks, platforms and devices can be made more secure.

Cellular connectivity is still improving, and smartphones and tablets are equipped with internal storage for holding data such as EHR or EMR. Cellular technology used for mHealth will, in the future, be expected to function in real time, so data latency—the time taken to collect and store the data—must be addressed from a security perspective.

Currently, cellular data networks are able to support VoIP or mVoIP and video, utilizing internet protocol (IP)-capable wireless network connections such as evolution-data optimized (EV-DO), HSPA+, and simultaneous voice and LTE (SV-LTE). However, they have no dedicated channels for medical device transmissions, primarily due to cost.

Such networks are generally deemed to be reliable, but there are instances where data transmissions could fail (for example, when transmitting data from a patient under remote supervision). If the data network path reassembles the message with a significant delay, there is the possibility of untenable latency with real-time applications. When addressing such issues from a safety and security perspective, the third generation partnership project (3GPP) standard should be among the options considered.

Device data capabilities specifically for merging cellular technology such as LTE with multiple bandwidths, require manufacturers to understand the network providers' throughput limitations. For this reason, there are organizations such as the 3GPP, the Wireless Association

(CTIA), Global Certification Forum (GCF), and PCS Type Certification Review Board (PTCRB) that help to ensure a baseline of quality of service (QoS) for reliability of connection and latency.

Data Collection Software and Apps

In addition to proprietary products, open-source licenses for healthcare software are available, in which the source code is made available for anybody to use, and can usually be freely modified for custom purposes. Open-source licenses are commonly free of charge, but sometimes have relatively minor licensing limitations.

While open-source licensing facilitates customized product development and its rapid placement in the market, there is a potential safety concern with the use of this software from the perspective of its robustness and compatibility.

Open-source licenses are presently available for some of the following types of software:

- Bio surveillance and public health: statistical and epidemiological studies[9,10]
- Dental: patient records and dental management[11]
- EHR and EMR (electronic health and medical records)[12-14]
- Imaging[15-17]
- Management of health systems[18]
- Management of medical practice[19]
- Medical information systems[20]
- Mobile devices[21,22]

Building Blocks for Sustainable and Scalable mHealth Approaches

Today we are at a critical juncture in healthcare development: There will either be a breakthrough toward development and acceptance of new trends and the technologies needed for mHealth, or expectations will not be met. Based on development in other sectors, technology seems not to be the limiting factor. The success or failure of healthcare will depend heavily on the position and interests of the major healthcare stakeholders, namely government (including regulators), industry, and users.

As we have seen, mHealth does not just involve remote direct communication between patient and healthcare worker. There are many other emerging trends that should be considered, such as:

- Clinical decision support
- Alarm and emergency response systems (e.g. emergency hospital care, traffic, and accidents)
- Quality and verification of pharmaceutical supply chain integrity
- Human-resources management and supervision
- Monitoring and reporting of performance of healthcare services
- Continuous education and professional development for healthcare workers
- Specific health community mobilization
- Support of self-health management, particularly for long-term or chronic conditions

Today we are at a critical juncture in healthcare development: There will either be a breakthrough toward development and acceptance of new trends and the technologies needed for mHealth, or expectations will not be met.

Standardization and Regulation

At present, there are some general approaches for attempting to establish interoperability of medical devices and information systems, including but not necessarily limited to:

(a) **Proprietary systems**, in which individual vendors ensure interoperability by constraining system integration via proprietary messaging and interfaces
(b) **Drivers** that allow for interface across multiple proprietary components
(c) **Centralized translators** that serve as a coordinating hub across multiple disparate platforms
(d) **Specific system architectural requirements** or constraints through architectural standards

A number of standards, profiles, or collaborations have been developed or are currently under development to address various aspects of medical devices interoperability, including, but not limited to:

- ASTM F2761-09 for the integrated clinical environment
- Digital imaging and communications in medicine (DICOM)
- Health level 7 (HL 7)
- IEEE 11073 medical device communication standards
- Integrating the healthcare enterprise (IHE)
- Medical device interoperability coordination council (MDICC)
- Continua Health Alliance standards, design guidelines, and reference architectures
- UL 2800 for interoperable medical device interface safety

Some standards may become critical to the convergence of conformance with regulations, in part driven by the U.S. Food and Drug Administration (FDA) and industry approach to medical devices. As medical devices interface with medical device data systems (MDDS), EMR, EHR, and a variety of regulated and unregulated pieces of information technology (IT) infrastructure, there is a need to further define what constitutes a 'medical device.'

Industry is increasingly interested in understanding and addressing the risks and safety considerations of mHealth systems and environments. These include medical devices, information technology (IT) components, networking, and (IT) infrastructure, areas that have up to now been relatively or entirely unregulated, particularly with respect to cybersecurity.

Industry is increasingly interested in understanding and addressing the risks and safety considerations of mHealth systems and environments.

The FDA's definition of MDDS (2011 Final Rule) is one of several efforts underway to clarify complex mHealth issues, and together with "Draft Guidance for Industry and Food and Drug Administration Staff—Mobile Medical Applications," also released in 2011, will begin to set the stage for the future of mHealth.

As software, as a stand-alone product, begins to fall into the realm of safety standards that were previously focused on software embedded within physical products, we will begin to see a significant shift in how safety-related apps, libraries, operating systems, development tools, and even models and algorithms are viewed by regulators and certification organizations.

Safety and Security

There are two main perspectives of mHealth safety: The potential for improvement of public health and safety through mHealth technologies (as discussed above); and for compromising the existing level of basic safety, essential performance, or security of networked medical devices. Basic safety, essential performance, and security can be compromised via three main mechanisms:

(a) **Random faults** whose probability is increased by introducing large volumes of network data and accompanying electrical stresses. These faults may cause malfunction through, for example, lost or corrupted data (whose absence may result in harm), or data that is randomly altered, triggering potentially harmful 'normal' operating states of the equipment.

(b) **Systematic faults** whose probability is increased by unforeseen network or system integration stresses that exceed device design limitations. An example of a systematic fault would be the mismatched units of measure in the Mars Climate Orbiter's inflight and ground control software.[23]

(c) **Malicious attack**, a subset of systematic faults that occurs via security vulnerabilities. Between January 2009 and May 2011, the Department of Veterans Affairs tracked 173 medical devices infected with malware.[24] Such findings help confirm FDA concerns raised in their 2005 "Guidance for Industry—Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software," in which the consequences of not addressing the vulnerability of networked devices that use software are described.

Moving Forward

The many benefits of connecting mobile medical devices are clear, and the technologies needed for mHealth implementation are emerging. However, there are still hurdles to be overcome. It is now up to the suppliers, developers, integrators, regulators, standards-writers, educators, and certifiers to work together as a community toward a unified goal: the development of an interoperable, safe mHealth ecosystem. ■

References

1. **Istepanian R, Laxminarayan S, and Pattichis CS.** *M-Health: Emerging Mobile Health Systems.* Springer Science & Business Media; 2006.

2. **Torgan C.** The mHealth Summit: Local & Global Coverage. November, 2009. Kinetics. Available at: www.caroltorgan.com/mHealth-summit/. Accessed Aug. 9, 2012.

3. **ITU.** Standards and eHealth: ITU-T Technology Watch Report January 2011. International Telecommunication Union. Available at: www.itu.int/dms_pub/itu-t/oth/23/01/t23010000120003pdfe.pdf. Accessed Aug. 9, 2012.

4. **Swedish Presidency of the European Union.** eHealth for a Healthier Europe—Opportunities for a Better Use of Healthcare Resources. Available at: www.se2009.eu/polopoly_fs/1.8227!menu/standard/file/eHealth%20for%20a%20healthier%20europe.pdf. Accessed Aug. 9, 2012.
5. **Electronics.ca Publications.** Wireless Health Market: Global Trends, Opportunities, Competitive Landscape and Forecasts to 2016. Available at: www.electronics.ca/publications/products/wireless-health-market%3a-global-trends%2c-opportunities%2c-competitive-landscape-and-forecasts-to-2016.html. Accessed Aug. 9, 2012.
6. **Vital Wave Consulting.** *mHealth for Development: The Opportunity of Mobile Technology for Healthcare in the Developing World.* Washington, D.C. and Berkshire, UK: UN Foundation-Vodafone Foundation Partnership, 2009.
7. **UN.** We Can End Poverty: 2015 Millennium Development Goals. United Nations. Available at: www.un.org/millenniumgoals/bkgd.shtml. Accessed Aug. 9, 2012.
8. **PricewaterhouseCoopers.** *Emerging mHealth: Paths for Growth.* June, 2012. Available at: www.pwc.com/gx/en/healthcare/mHealth/index.jhtml?wt.ac=vt-mHealth#&panel1-1. Accessed Aug. 9, 2012.
9. **CDC.** Introducing Epi Info 7. Centers for Disease Control. Available at: wwwn.cdc.gov/epiinfo/. Accessed Aug. 9, 2012.
10. **Eclipse.** The Spatiotemporal Epidemiological Modeler (STEM) Project. Available at: www.eclipse.org/stem/. Accessed Aug. 9, 2012.
11. **Open Dental.** Open Source License. Available at: www.opendental.com/manual/openlicense.html. Accessed Aug. 9, 2012.
12. **Mobile Health News.** Berg: 2.2M Patients Remotely Monitored Globally. Available at: http://mobihealthnews.com/15487/berg-2-2m-patients-remotely-monitored-globally/. Accessed Aug. 9, 2012.
13. **Communi.** CommuniMed. Available at: www.communi.com.br/communimed. Accessed Aug. 9, 2012.
14. **GNU Health.** GNU Health: The Free Health and Hospital Information System. Available at: http://health.gnu.org/. Accessed Aug. 9, 2012.
15. **Open EMR.** Open EMR. Available at: www.open-emr.org/. Accessed Aug. 9, 2012.
16. **OsiriX Imaging Software.** OsiriX Imaging Software. Available at: www.osirix-viewer.com/. Accessed Aug. 9, 2012.
17. **SourceForge.** Xebra: Beta. Available at: http://sourceforge.net/projects/xebra/. Accessed Aug. 9, 2012.
18. **Endrov.** E:Endrov. Available at: www.endrov.net/wiki/index.php?title=main_page. Accessed Aug. 9, 2012.
19. **iHRIS.** iHRIS: Free and Open Health Workforce Information Software. Available at: www.ihris.org/. Accessed Aug. 9, 2012.
20. **FreeMED.** FreeMED: Open Source Electronic Medical Record Software. Available at: http://freemedsoftware.org/. Accessed Aug. 9, 2012.
21. **CAISIS.** Integrated Clinic and Research Management System (CAISIS). Available at: www.caisis.org/. Accessed Aug. 9, 2012.
22. **Roll Back Malaria Partnership.** SMS for Life: An RBM Initiative. Available at: www.rbm.who.int/psm/smswhatIsIt.html. Accessed Aug. 9, 2012.
23. **Beatty S.** Sensible Software Testing. Embedded Systems Programming. 2000;8.
24. **Healthcare Info Security.** Medical Device Security Raises Concerns: Malware Poses Risk to Patient Safety. Available at: www.healthcareinfosecurity.com/articles.php?art_id=3644. Accessed Aug. 9, 2012.