Achieving Global Approval for mHealth Devices and Products
The adaptation of wireless technologies is a key element in the overall effort by healthcare providers and caregivers to increase access to services, improve patient outcomes, control costs and provide patients with greater mobility. As such, mobile medical technologies represent a clear and significant opportunity for manufacturers seeking to provide products and services to an increasingly dynamic and complex healthcare marketplace. Indeed, the global market for wireless health technologies is projected to reach more than $38.5 billion by 2016, representing an average annual growth of nearly 20%.1

Despite their growing use in healthcare settings, however, mobile technologies present a number of unique safety and security concerns that go beyond those found with similar devices used in other environments. In a worst-case scenario, an equipment or software malfunction or interoperability issue can directly result in life-threatening consequences for patients or healthcare providers. In other cases, electromagnetic interference (EMI) can cause device immunity issues leading to inaccurate data transmission or misdiagnosis of a patient’s condition and inappropriate treatment. Mobile systems are also potentially vulnerable to malicious cyber interrogation, with consequences ranging from inappropriate exposure of confidential personal health record (PHR) or electronic health record (EHR) of patient’s data to unreliable equipment performance.

The convergence of wireless technologies and medical devices (also called mobile health or mHealth) presents new technological challenges and increased regulatory scrutiny. This is particularly true in the U.S. and other jurisdictions where rigorous third-party product approval processes are mandatory.

This UL white paper provides an overview of mHealth technologies and the regulatory requirements that manufacturers must address before bringing new mHealth devices to market. Beginning with a general background on mHealth technologies, the paper then discusses specific safety and security risks associated with their use. The white paper then provides a framework for the various technical issues associated with mHealth technologies, and discusses specific regulatory requirements in key markets around the world. The paper concludes with recommendations for manufacturers seeking global approval for mHealth technologies.
The Role of mHealth Technologies in Today’s Healthcare System

The healthcare industry is currently undergoing an unprecedented transformation as healthcare providers are under pressure to increase access and reduce costs while improving the quality of patient care. As part of the broader effort to achieve these goals, healthcare institutions are making significant investments in advanced information and communications technologies designed to support the collection and reporting of critical patient data. The resulting PHRs and EHRs equip healthcare providers with real-time information that can improve the quality and timeliness of patient care while also increasing operational efficiencies that can reduce the cost of care.

In this white paper, mHealth is defined as the provision of healthcare services through the medium of mobile communications devices. These technologies are playing an important role in the overall effort to collect and maintain accurate and consistent patient data. Clinicians now use tablet computers, so-called smart phones and other devices to record and retrieve vital patient information in real time. Wireless monitoring equipment that reads and records patient vital signs such as heartbeat and blood pressure can automatically transmit data to tablet computers or smart phones via any number of wireless network technologies, seamlessly updating patient records. These and other electronic devices operate through specialized software applications designed to facilitate data exchange among various platforms.

The use of mHealth technologies provides multiple benefits to patients, healthcare professionals and healthcare institutions. Devices and products based on mHealth technologies can automatically update relevant PHRs and EHRs in real-time, thereby providing healthcare professionals with the most current patient medical data and increasing the efficiency and effectiveness of patient monitoring and treatment. Such devices also provide patients with greater mobility and independence, allowing them to resume everyday activities outside of the traditional healthcare settings or to receive medical evaluation and treatment in remote locations. Healthcare institutions deploying mHealth services can improve the overall quality of patient care while also optimizing resource utilization and the use of caregivers.

These benefits are expected to drive growth in the market for mHealth devices and products in the coming years. One projection estimates that the global market for wireless medical technologies will grow nearly 20% a year between now and 2016, from just over $16 billion in 2011 to over $38 billion by 2016.2 A separate study estimates that over 40,000 separate mobile healthcare software applications are currently available, and that annual mobile app downloads will increase from 44 million in 2012 to 142 million by 2016.3 Clearly, mHealth presents a significant opportunity for manufacturers and distributors of medical devices and software applications.

Safety and Security Issues for mHealth Technologies

Despite their significant benefits, mHealth technologies present a number of potential safety and security concerns. These concerns can adversely impact the accurate collection and integrity of patient data, and even expose patients and healthcare workers to certain health and safety risks. Here are some of the key issues and concerns related to the use of mHealth technologies:

- Interoperability with other wireless medical devices — The effectiveness of medical technologies in general and mHealth technologies in particular depends on the extent to which they can consistently and reliably exchange data with other medical devices. Yet, according to at least one study, although 90% of hospitals use six or more types of medical devices that could be integrated with their EHRs system, only one out of three hospitals actually do so. The waste and inefficiency associated with lack of interoperability carries an estimated annual cost of over $30 billion in the U.S. alone.5

- Electromagnetic interference (EMI) and immunity — As the use of both medical and nonmedical wireless devices increases, so too does the potential for unintentional interference caused by radio frequency (RF) emissions. Devices utilizing radio frequency (RF) technology have the potential to unintentionally affect the function of other medical devices.
Similarly, emissions from other medical and nonmedical devices can unintentionally affect the operations of mHealth devices. These unintended effects can include distortion or corruption of data being transmitted, reductions in the speed of device performance or blocking of communications signals, and can result in increased error rates, unsuccessful device initiation or termination of an intended operation.

- Human exposure to electromagnetic radiation (EMR) — Prolonged exposure to nonionizing radiation presents a potential risk to the health and safety of both patients and healthcare workers. High power radio frequency (RF) transmitters can produce energy that is absorbed in human tissues in close proximity, potentially producing a range of adverse effects, including but not limited to heating. This can be a particular concern for medical devices incorporating wireless technologies that are used in close proximity to patients or staff. Past research in this area has focused primarily on risks associated with the use of handheld phone, but additional research into the general effects of EMR is ongoing.

- Data integrity and security — Like most electronic technologies connected to the Internet or a wireless network, mHealth technologies are potentially vulnerable to cyber attack, either through malware, virus-corrupted messages or malicious activities. Computer malware has reportedly infected at least 327 medical devices at VA hospitals since 2009, according to the U.S. Department of Veterans Affairs. Cyber attacks can not only impact patient safety, but can also result in breaches that compromise the security of EHR systems and the release of confidential patient information.

### The Technical Framework for mHealth Standards and Regulations

Regardless of where they are marketed or sold, mHealth technologies, devices and applications are typically subject to a review and evaluation of the product’s compliance with minimum safety and operational specifications. Existing or proposed standards and national requirements applicable to mHealth already address some or all of the following technical criteria:

- **Wireless functionality** — Wireless technology is a critical component of mHealth devices. Primary wireless technologies include Bluetooth and Bluetooth Smart for devices utilizing wireless personal area networks (WPANs) body area networks (BANs), and Wi-Fi, 3G high speed packet access (HSPA) and others for devices utilizing wireless wide area networks (WWANs). Regardless of the wireless technology involved, mHealth devices incorporating wireless technology are subject to both qualification according to industry standards and regulatory type approvals.

- **Radio frequency performance** — As previously noted, the operation of mHealth devices can cause unintentional interference with other electrical and electronic devices. Devices and products utilizing mHealth technologies are also susceptible to RF interference generated by other electrical and electronic equipment. Most countries mandate threshold RF performance requirements to minimize potential interference and reduce RF susceptibility.

- **Product safety** — In most countries, mobile medical devices are subject to the same product safety requirements as non-mobile medical devices. These requirements include electrical safety shock and hazard testing, and may also include an assessment for functional safety. Manufacturers of mHealth devices may also be required to comply with the risk management requirements found in IEC 60601, 3rd edition. Wireless medical devices are also subject to RF exposure evaluation to assess potential health and safety effects, and specific absorption rate (SAR) measurements and maximum permissible exposure (MPE) assessments are often required.

- **Device and data interoperability** — Device interoperability is an
emerging trend in the evaluation and qualification of mHealth technologies and other medical devices. Numerous initiatives are underway to promote device interoperability through the adoption of industry-wide standards. As an example, UL, in conjunction with the Association for the Advancement of Medical Instrumentation (AAMI), has embarked on the development of a suite of standards intended to create an interoperability implementation framework that addresses potential safety issues. In addition, the Continua Health Alliance is promoting interoperability for assisted living devices by consolidating aspects of international standards into a guidance document for manufacturers.

- Other considerations — mHealth devices may also be subject to testing for immunity to electrostatic discharge (ESD), since ESD events can result in device malfunction or failure.

It is important to note that tablet computers, smartphones and certain other electronic devices with wireless capabilities that are primarily intended for commercial applications or for use by consumers may also be classified as medical devices by regulatory authorities when used in a healthcare environment. As such, they may be subject to additional evaluation and testing according to the standards and requirements applicable to medical devices. Manufacturers of such devices should be mindful of the potential need to meet additional compliance requirements when evaluating and selecting target markets.

The Regulatory Framework for mHealth Technology Acceptance

Within the context of the technical framework described in the previous section of this paper, specific regulations for mHealth technologies vary from country to country. The regulatory approval scheme for mHealth devices is most fully established in the U.S. and the European Union (EU), and compliance with the regulatory requirements in these jurisdictions can ease the path toward product acceptance in other countries. However, despite efforts to achieve global harmonization, regulations applicable to mHealth devices sold or marketed in other countries may deviate in important respects.

The following sections provide an overview of regulatory considerations applicable to mHealth technologies in the U.S., the EU and other selected countries.

United States

All medical devices sold or marketed in the U.S. must comply with mandatory product safety regulations and a registration process administered by the U.S. Food and Drug Administration.
Achieving Global Approval for mHealth Devices and Products

Achieving Global Approval for mHealth Devices and Products

Manufacturers and importers must register their companies with the FDA, and foreign manufacturers must designate a U.S.-based representative. All medical devices must be listed with the FDA, and certain devices are subject to premarket approval by the agency under its 510(k) program.

Although the FDA doesn’t directly regulate wireless devices, it has issued a guidance document “Radio-Frequency Wireless Technology in Medical Devices,” intended to provide manufacturers and importers with recommendations on addressing essential safety issues related to the function and operation of wireless medical devices, including mHealth devices. Specifically, the guidance document discusses the importance of evaluating the electromagnetic compatibility (EMC) of any RF wireless medical device submitted for FDA approval. The guidance document also recommends the application of risk management principles to address the FDA’s design control requirements.

European Union

Requirements applicable to wireless device in the U.S. are expressly regulated by the U.S. Federal Communications Commission (FCC), and codified in Section 47 of the U.S. Code of Federal Regulations (CFR 47), Parts 15 and 68. The FCC requires emissions testing to verify that a device cannot cause harmful interference with other electrical or electronic equipment or communications network, and immunity testing to assess whether device performance degrades when exposed to electromagnetic interference. The FCC also requires SAR testing to verify that RF emissions from radio devices do not exceed maximum permissible levels.

One other area of regulatory consideration in the U.S. is the FDA’s draft guidance, “Mobile Medical Applications.” published in 2013, the guidance is intended to provide direction to the emerging mobile medical application market on the use of dedicated software applications on mobile platforms.

As with electronic devices primarily intended for commercial or consumer use, application developers should be careful to assess whether their software could be construed as a medical application, thereby subjecting it to FDA oversight.

European Union

Regulations in the EU applicable to mHealth technologies are found in EU directives and published standards. Directives describe “essential requirements,” which are transposed into the national law of EU Member States, while published standards provide detailed technical specifications. Manufacturers and importers of devices that are in compliance with the essential requirements of all applicable directives may apply the CE Mark to their products as evidence of conformity, and legally market and sell their products in each EU Member State without further testing.

EU requirements applicable to mHealth technologies and devices can be found in the following directives:

• Radio & Telecommunications Terminal Equipment (R&TTE) Directive (1995/5/EC): This Directive applies to all products and devices that utilize the radio frequency spectrum for wireless communications, as well as those devices that connect to public telecommunications networks. Compliance with the R&TTE Directive’s requirements typically involves testing and verification by an EU Notified Body.

• Electromagnetic Compatibility (EMC) Directive (2004/108/EC): The EU’s EMC Directive applies to all electrical and electronic equipment that generates electromagnetic interference (intentional or unintentional). In that regard, the EMC Directive parallels the FCC’s Part 15 EMC requirements in the U.S. Compliance with the Directive’s requirements is typically demonstrated by a declaration of conformity issued by a manufacturer or importer, and based either on in-house testing or testing conducted by a third party.

• Low Voltage Directive (2006/95/EC): The Low Voltage Directive (sometimes referred to as the LVD) provides essential product safety requirements for any electrical or electronic equipment operating within specific voltage limits. Compliance with the LVD is usually demonstrated by a declaration of conformity issued by the manufacturer or importer, and based either on in-house testing or testing conducted by a third party.

• Medical Device Directive (93/42/EEC) and Directive on Active Implantable Medical Devices (90/385/EEC): The EU’s Medical Device Directive and its Directive on Active Implantable Medical Devices (collectively known as
Achieving Global Approval for mHealth Devices and Products

MEDDEVs), detail essential safety requirements for medical devices and implantable medical devices. Demonstrating conformity with the requirements of these Directives depends on the class of medical device being evaluated, and ranges from a manufacturer’s declaration of conformity to testing by an EU Notified Body. For most medical devices, the Directives also require manufacturers to maintain a quality management system, and to conduct a full risk management assessment as part of the evaluation process.

Canada

In Canada, wireless devices are regulated by Industry Canada, and technical requirements are similar to those of the U.S. FCC. Generally, manufacturers can submit data from FCC testing in connection with their application for Canadian approval, although some additional testing may be required. Manufacturers based outside of Canada are also required to designate a Canadian-based representative.

The Therapeutic Product Directorate of Health Canada is Canada’s government agency responsible for the regulation and oversight of medical devices. Under Canada’s regulations, medical electric devices are organized into one of four classes based on their potential risk to patients. Manufacturers of any medical device categorized as Class II, III or IV must obtain a medical device license prior selling that device in the Canadian market. Medical device manufacturers are also generally required to maintain a quality management system, which is subject to third-party auditing and certification.

Japan

Wireless devices sold or marketed in Japan fall under the jurisdiction of the Japan Approvals Institute for Telecommunications Equipment (JATE). Product testing and certification by an approved certification body is required before a device can be legally marketed. Testing is based on IEC standards, and data from CE Mark testing is generally accepted.

Medical devices are subject to the requirements of the Japan Pharmaceutical Affairs Law (PAL), as administered by Japan’s Pharmaceutical and Medical Devices Agency (PMDA). Medical devices are categorized according to the degree of risk they present to a patient or user, and premarket approval is generally required before a device can be legally sold in Japan. Medical device manufacturers not based in Japan must also appoint a marketing authorization holder (MAH) licensed by Japan’s Ministry of Health, Labor and Welfare to manage the device registration process.

China

Wireless devices must be certified by China’s Certification and Accreditation Administration (CNCA) and granted approval to use the China Compulsory Certification (CCC) Mark prior to being placed on the market. Compliance testing is conducted exclusively by CNCA-designated testing laboratories based in China and factory inspections are also part of the certification process.

Medical devices are subject to regulation by China’s State Food and Drug Administration (SFDA), and all imported medical devices must obtain a device registration certificate from the SFDA. Manufacturers seeking device registration must have their device tested to applicable national or industry standards by an approved testing laboratory based in China.

Global Harmonization Efforts

Created in 2011, the International Medical Device Regulators Forum (IMDRF) is a voluntary group of representatives from regulatory authorities in various countries working to accelerate the harmonization of national medical device regulations and requirements. Representatives from the U.S., the EU, Canada, Japan, Australia and Brazil are members of the IMDRF Management Committee. (As of this writing, the memberships of China and the Russian Federation are being confirmed.)

Current IMDRF working group programs include creating a list of international standards to be used for the evaluation of medical devices, and the development of a standard set of requirements for organizations that conduct mandatory audits of manufacturers’ quality management systems. As the work of the IMDRF progresses, it is anticipated that other countries will strive to harmonize their own regulations affecting medical devices with those of IMDRF member countries.
At present, a similar global harmonization effort applicable to wireless technologies does not exist. However, the regulation of devices using wireless technologies is largely based on technical specifications found in internationally accepted standards, such as those produced under the auspices of the International Electrotechnical Commission (IEC) and the Institute of Electrical and Electronic Engineers (IEEE). In addition, technology qualification programs such as the Bluetooth® Qualification Program provide objective technical criteria that can be adopted by regulatory authorities.

The Approval Path to Global Compliance

Because of their design and intended use, mHealth technologies must comply with the technical requirements applicable to electrical and electronic equipment, wireless communications devices and medical devices. In evaluating compliance with wireless requirements alone, a single mHealth device would likely be subject to the following:

- Specific absorption rate (SAR) testing
- Radio frequency (RF) performance testing
- Bluetooth testing
- Electromagnetic compatibility (EMC) testing
- Device interoperability testing
- Device co-existence testing

Applicable testing requirements are further complicated by global standards and national regulatory processes that are only partially harmonized. For example, an mHealth device manufacturer might be required to conduct a specific test multiple times to demonstrate compliance with varying requirements set by national regulations, or to perform some tests for compliance with one country’s requirements but not others.

These complexities create significant challenges for manufacturers, importers and distributors of mHealth technologies seeking access to global markets for their products.

The best approach for achieving global compliance as efficiently and as cost-effectively as possible is to consult early in the product planning and design process with compliance and testing professionals who have technical expertise in every aspect of mHealth technologies, as well as experience in the regulatory approvals process of the targeted national markets. Initial planning can result in more robust product designs that account for every compliance contingency, reducing the need to implement problematic design changes late in the product development process. These advantages can result in a shorter product development process, the more rapid deployment of new technologies to market, and an important competitive edge.
Summary and Conclusion

As more medical devices incorporate wireless capabilities, mHealth technologies will transform healthcare by improving the timeliness and accuracy of patient information, reducing costs and improving the care of patients regardless of their location. However, because of their design and intended use, mHealth technologies are subject to a wide range of different technical requirements, a challenge further complicated by a lack of harmonized standards and regulatory approval processes that differ from country to country.

Manufacturers of mHealth technologies can minimize these challenges by proactively planning a global compliance strategy at the very earliest stages of new product development. This approach can eliminate the need for design changes late in the development process, and reduce regulatory approval delays due to noncompliance.

UL offers a complete range of testing services for mHealth technologies, and has a comprehensive knowledge of the regulatory approval process in key target markets. For additional information, please contact our expert team at Medical.Inquiry@ul.com.