

# **A Call for Clarity: Open Questions on the Scope of FDA Regulation of mHealth**

**A whitepaper prepared by the mHealth Regulatory Coalition**

December 22, 2010

## **Authors**

Bradley Merrill Thompson  
Epstein, Becker & Green P.C.  
Washington, D.C.  
bthompson@ebglaw.com

Leah Kendall  
Epstein, Becker & Green P.C.  
Washington, D.C.  
lkendall@ebglaw.com

M. Jason Brooke  
Epstein, Becker & Green P.C.  
Washington, D.C.  
jbrooke@ebglaw.com

Dane Stout  
Anson Group, L.L.C.  
Indianapolis, IN  
dstout@ansongroup.com

# Introduction

The mHealth Regulatory Coalition (referred to subsequently as the Coalition) is comprised of industry representatives that manufacture and distribute the fundamental hardware and software used in mHealth\* systems, healthcare providers who use mHealth technologies to improve healthcare delivery, and non-profit organizations that advocate on behalf of patients and providers for the use of mHealth in the United States.

In this whitepaper, the Coalition analyzes two fundamental questions: (1) what mHealth hardware and software will the U.S. Food & Drug Administration (subsequently referred to as the FDA or the Agency) regulate and (2) if such products are regulated, in what device classification will the FDA place them? The three device classifications determine, among other things, whether a given product requires some sort of premarket clearance or approval from the FDA. The Coalition tackles these questions because, quite simply, the answers are fundamental to the business planning process and companies as well as investors need answers as soon as possible to maintain innovation.

The Coalition wrote this whitepaper after having spent nearly five months meeting internally, and with entrepreneurs and established companies alike, to learn about their mHealth business plans. Through this process, we identified the specific open questions to determine whether the FDA would regulate their products and any applicable classification. The Coalition's mission is to drive the analysis to a level of specificity that would be meaningful to the FDA.

Importantly, *this whitepaper does not attempt to solve these problems*. Rather, the Coalition focuses on defining the myriad of problems and challenges that arise when attempting to apply current FDA policies and requirements to the future landscape of mHealth technologies. The Coalition believes that both the mHealth industry and the Agency must first clearly define the issues before we can resolve them.

The goal of the mHealth Regulatory Coalition is to work with the FDA to develop and draft a guidance document that addresses the regulation of mHealth technologies, specifically identifying what aspects of mHealth are not regulated by the Agency. We believe that the development of a guidance document will bring greater clarity and predictability to the regulatory pathway for the numerous hardware and software components on which mHealth technologies rely. Through active engagement with the FDA in this process, the mHealth Regulatory Coalition—in alignment with the Agency's dual mandates—hopes to foster innovation while ensuring the safety and effectiveness of the products that will drive the future of the American healthcare system.

This whitepaper moves us one step closer to completing our goal, by ensuring a common understanding of the nature and contours of the problem. By the end of the first quarter of 2011, we intend to prepare a guidance document that proposes solutions to the questions presented here.

---

\* The *m* in *mHealth* is an abbreviation for *mobile* to recognize the the integration of mobile technology in healthcare today.

## Structure of the Whitepaper

This whitepaper is written such that each chapter addresses a particular aspect of mHealth regulation. Chapter 1 provides an overview of the problems that developers of mHealth technologies face given the current regulatory framework. Chapters 2–4 have two primary purposes: 1) to describe our current understanding of FDA regulation of mHealth; and 2) to provide a broad industry perspective on the challenges posed by the existing regulatory environment. Specifically, the subsequent chapters discuss the following:

- **INTENDED USE:** Whether a product will be regulated as a medical device depends on the product’s intended use, including any indications for use. In the mHealth area, there is sometimes a grey area between general health and wellness on the one hand and diagnosis or treatment of a disease or health condition on the other. This makes determining the intended use challenging. Chapter 2 examines current requirements and interpretations surrounding “intended use” and highlights the challenges by considering several examples of connected devices that can serve medical or wellness purposes, sometimes simultaneously.
- **mHEALTH COMPONENT CONFIGURATIONS AND THE DEVICE-ACCESSORY CONNECTION:** Chapter 3 examines the implications of the FDA’s device accessory classification policy as applied to mHealth configurations. To understand this particular challenge, we discuss some of the likely interconnections used among the various components that comprise the overall mHealth system. Such components could include:
  - a. Already-classified medical devices with an established medical purpose and use;
  - b. Sensors, actuators, and chipset connections necessary for enabling mHealth, including direct machine-to-machine (M2M) interactions between medical devices and a data capture device worn or carried by the patient;
  - c. Smartphone and Web applications (or “apps”) that support medical device interaction or in some cases, that serve a medical device function themselves;
  - d. Smartbooks, netbooks, tablets, and other new devices used by people and potentially connected to medical devices;
  - e. Handset manufacturer and home Wireless Gateways; and
  - f. Network access points, carriers, and Internet-based software.
- **SOFTWARE FUNCTIONALITY:** Chapter 4 examines the FDA’s current software rules and the ambiguities that arise when determining when and where software used in mHealth becomes a medical device. This could include software deployed at a body area network (BAN) or personal area network (PAN) level, software on a mobile phone or home gateway, an electronic health record (EHR)<sup>†</sup> with software that processes incoming medical device data, or larger clinical

---

<sup>†</sup> Throughout this whitepaper, we use the terms *electronic health record (EHR)*, *personal health record (PHR)*, and *electronic medical record (EMR)*. Elsewhere these terms are used both interchangeably and for specific purposes. It is important to recognize that these three terms have distinct meanings. An EMR is used exclusively by a single healthcare provider (e.g., hospital or ambulatory care facility) as the legal record of a patient’s health information. An EHR is an amalgamation of data sourced from EMRs from a patient’s various healthcare providers. A PHR consists of patient data that are generated and

decision support software running remotely and accessed through a network connection using data collected from mHealth devices.

Everyone—including the FDA—wants to see innovation in mHealth. To see 1,000 ideas blossom, however, industry needs some clarity regarding the scope of the FDA’s requirements going forward in each of these areas. Business people simply have to know whether compliance with the FDA regulations needs to be part of their plan. Clarity and predictability are critical to continued innovation in mHealth. The FDA has previously announced that it is working on its own guidance document to offer some general advice on how mHealth apps are regulated, including what needs to be in a premarket submission. It is difficult to predict when new policy will emerge from the Agency. As anyone who has followed the proposed medical device data system rule knows, it can take years. The Coalition’s hope is that the FDA will find this whitepaper useful in moving that process along.

---

entered by the patient and can incorporate data from both EMRs and EHRs. We use these terms in accordance with the definitions above.

# Executive Summary

This whitepaper outlines the myriad of specific questions that underlie two fundamental questions: (1) what mHealth hardware and software will the U.S. Food & Drug Administration (FDA) regulate and (2) if such products are regulated, in what device classification will the FDA place them?

Many of the questions arise because certain FDA policies were written decades ago at a time when our understanding of the connections between lifestyle and disease were not well-understood. This is not the first time the FDA has confronted such a challenge. In the early 1990s when scientists began to understand better the connections between dietary supplements and health, initially the FDA tried to regulate those supplements as drugs. At the time, the FDA's policies required that any health claims associated with ingested products triggered drug status. Fortunately, Congress and the FDA came up with a more nuanced regulatory solution that allowed dietary supplements to be brought to market without filing a new drug application.

A very significant number of mHealth products appear designed to help consumers make better choices in their lifestyles, thereby promoting healthy living. mHealth creates a connection that gives people better access to useful information when they need it wherever they are—where they live, where they work and where they play. That access to information allows consumers to take more control of their lives and make better decisions on such things as diet, exercise and avoiding conditions that stress their health. Just as with dietary supplements, it must be recognized that this new knowledge of connections between lifestyle and health should not cause innovative, low risk products to become over-regulated.

At a high-level, the Coalition's whitepaper focuses on questions that arise in three areas:

1. To what extent can mHealth-related products be excluded from FDA regulation by focusing their marketing campaigns on general improvements to consumer wellness, as opposed to focusing on the management or treatment of diseases such as diabetes and hypertension? For example, would the hardware and software associated with a system promoted for periodic transmission of a consumer's weight to his physician be a regulated medical claim or an unregulated wellness claim? What if the data are instead merely transmitted to a personal health record not associated with any particular physician? The Coalition generated a set of similar questions that all require clarification of the fine line between treatment of disease and promotion of wellness that defines FDA jurisdiction.
2. To what extent do mobile phones and other generic communication hardware become FDA regulated medical devices simply because they are promoted for connection to a medical device? Would a mobile phone manufacturer that does nothing more than passively sell through its online store a third-party app designed to connect the mobile phone to a blood glucose meter cause the mobile phone to become a regulated medical device? Would a mobile phone intended to be used to download data from a pacemaker become itself a Class III medical device and regulated to the highest degree? The FDA's so-called accessory policy that for decades has held that any product intended to be connected to a medical device is regulated to the same degree as the medical device produces some illogical scenarios if applied literally in today's connected health environment.

3. To what extent does the FDA regulate software apps that are intended to reside on mobile phones, ordinary PCs, servers or perhaps in the cloud if they function to provide connections between communication hardware and medical devices or as repositories for health data? For example, does the FDA intend to regulate personal health records? Is a software app stored on a mobile phone regulated as a medical device if it asks the patient questions and transmits the patient's answers to a health care provider? Does the FDA plan to regulate decision support software residing on a physician's mobile phone that offers a preliminary analysis of data received from the patient? Would software that sends a doctor an alert based on changes in a consumer's weight require prior clearance from the FDA? To what extent would software that the FDA intends to regulate require premarket notification? It has been years since the FDA clarified its stance on the regulation of software and today's mHealth systems heavily rely on software for a wide variety of functionality that requires clarity from the FDA on the appropriate level of regulation.

This whitepaper explains existing FDA policy in these three areas, answers at least at a high level the few questions that can be answered, and most importantly identifies the remaining open questions. This paper lays the foundation for the development of a guidance document that we plan to propose to the FDA, addressing the open questions. Basically, the Coalition first had to agree on the scope and nature of the problem to be solved, and then to suggest solutions to this problem.

# Chapter 1

## Charting the Future State of mHealth

The pace of change in the mHealth sector creates significant issues for policy makers and regulatory agencies as they attempt to evaluate the impact of mobile technology marketed or used for medical purposes. In the FDA context, mHealth-related technologies raise a host of pre- and post-market issues the most fundamental of which is the threshold question of which elements of the mHealth ecosystem the FDA will regulate. For that reason, this whitepaper focuses on *the scope of FDA regulation of mHealth products*.<sup>1</sup>

### Framing the Discussion: Defining mHealth for Use in an FDA Regulatory Context

Frequently the most difficult aspect of solving a complex problem is to build a *consensus opinion of precisely what the problem is*. To that end, we propose that the definition of mHealth for FDA regulatory purposes consist of the following elements:

1. Technology architecture; and
2. Software platforms and interfaces.

Below we discuss each of these elements and then provide a comprehensive list of “in scope” and “out of scope” technologies.

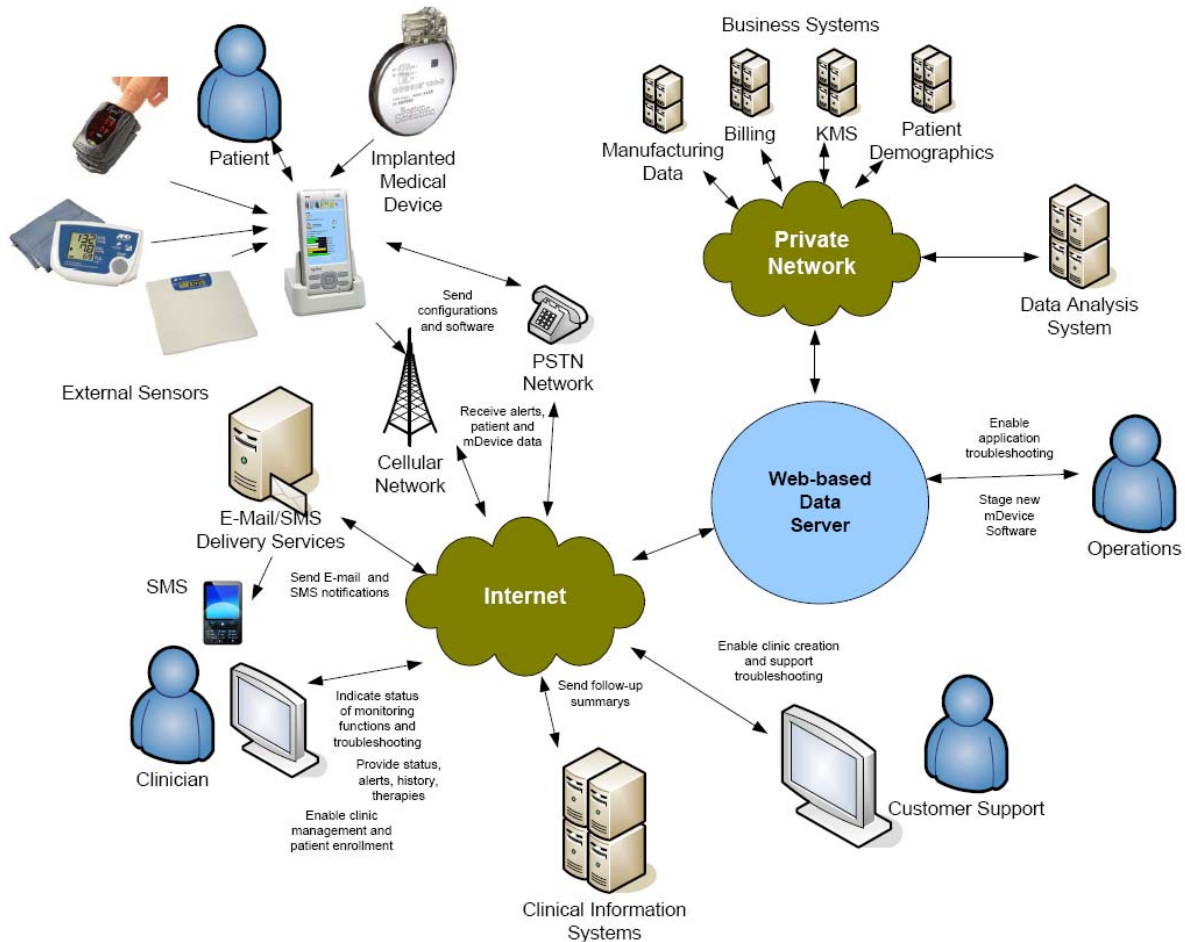
---

<sup>1</sup> There is much already written about the potential benefits and risks of using the existing and pervasive mobile phone and wireless infrastructures for healthcare purposes. In this whitepaper we attempt to avoid repeating what has already been well-documented, and instead refer readers to selected published articles and research. See generally ACCENTURE, INC., THE DAWN OF A NEW AGE IN HEALTHCARE: AN EARLY LOOK AT THE MARKET FOR NETWORKED DEVICES IN MHEALTH (2010), available at <http://www.slideshare.net/3GDR/accenture-mobile-healthcare-report>; DELOITTE CTR. FOR HEALTH SOLUTIONS, CONNECTED CARE: TECHNOLOGY-ENABLED CARE AT HOME (2008), available at [http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us\\_chs\\_ConnectedCare\\_final\\_0308.pdf](http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_chs_ConnectedCare_final_0308.pdf); GSMA & MCKINSEY & COMPANY, MHEALTH: A NEW VISION FOR HEALTHCARE (2010), available at [http://gsmworld.com/documents/mHealth\\_report.pdf](http://gsmworld.com/documents/mHealth_report.pdf); THE DIAGNOSIS FOR MEDICAL ELECTRONICS, EE TIMES (Dec. 2009), available at [http://www.nxtbook.com/nxtbooks/cmp/eetimes\\_medelectronics\\_20091207/index.php?startid=58#/1/OnePage](http://www.nxtbook.com/nxtbooks/cmp/eetimes_medelectronics_20091207/index.php?startid=58#/1/OnePage); PAUL H. KECKLEY & BIANCA CHUNG, DELOITTE CTR. FOR HEALTH SOLUTIONS, ISSUE BRIEF: THE MOBILE PERSONAL HEALTH RECORD: TECHNOLOGY-ENABLED SELF-CARE (2010), available at [http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Health%20Reform%20Issues%20Briefs/US\\_CHS\\_2010mPHR\\_091310.pdf](http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/Health%20Reform%20Issues%20Briefs/US_CHS_2010mPHR_091310.pdf); PWC HEALTHCARE RESEARCH INSTITUTE, HEALTHCARE UNWIRED (Sept. 2010), available at <http://pwchealth.com/cgi-local/hregister.cgi?link=reg/healthcare-unwired.pdf>; TIM SMITH & ROZ SWEENEY, NERAC, INC., FUSION TRENDS & OPPORTUNITIES: MEDICAL DEVICES AND COMMUNICATIONS (2010), available at [http://www.nerac.com/nerac\\_insights.php?category=reports&id=279](http://www.nerac.com/nerac_insights.php?category=reports&id=279); BRADLEY MERRILL THOMPSON, FDA REGULATION OF MOBILE HEALTH (2010), available at [http://mobihealthnews.com/wp-content/pdf/FDA\\_Regulation\\_of\\_Mobile\\_Health.pdf](http://mobihealthnews.com/wp-content/pdf/FDA_Regulation_of_Mobile_Health.pdf); Susannah Fox, *The Power of Mobile*, PEW INTERNET & AM. LIFE PROJECT (Sept. 13, 2010), <http://www.pewinternet.org/Commentary/2010/September/The-Power-of-Mobile.aspx>; Claudia Tessier, mHealth Initiative, The 12 mHealth Application Clusters (Feb. 3, 2010), <http://www.scribd.com/doc/27854061/The-12-mHealth-Application-Clusters>. These referenced materials are not intended to be exhaustive, but sufficiently representative.

## mHealth Technology Architecture

The technology architecture of an mHealth system can be complex, but the fundamental purpose is to provide the ability to change specific components without significantly impacting the overall performance and operation of the system. As discussed below, it is the balance of complexity and flexibility that makes an mHealth system powerful. To put this discussion into context, refer to Figure 1.1 as an example of the architecture of a single mHealth system.

**Figure 1.1:** An Example of Connected Hardware and Software in an mHealth System<sup>2</sup>

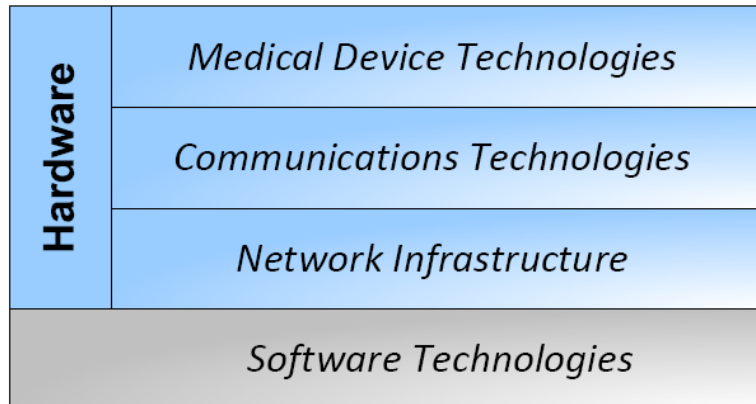


This Technology Architecture has been described as having four elements for the purpose of remote patient monitoring.<sup>3</sup> These four key elements also apply generally to mHealth technology, as described below.

<sup>2</sup> Courtesy of mHealth Regulatory Coalition Member, Boston Scientific Corp.

<sup>3</sup> SMITH & SWEENEY, *supra* note 1 (explaining the four key elements in the context of remote patient monitoring).

**Figure 1.2:** The Four Key Elements of an mHealth System



As shown in Figure 1.2, these elements are:

*1) Medical Device Technologies*

- Approved medical devices currently in use that require “communications enablement” but otherwise are used as originally intended;
- New submitted device indications, or new devices, that have clear intended medical use under existing regulatory policy; and
- New sensors and combinations of devices that rely on close patient proximity and direct data capture from automated monitoring or directed input by the patient.

*2) Communications Technologies*

- Wireless transmission protocols and equipment used within and to support multiple, end-use device types including:
  - Human-machine device interaction including personal computers, mobile phones, smartphones, personal digital assistants (PDAs), tablets, the plain old telephone service (POTS, or PSTN, the Public Switched Telephone Network), and other devices with interfaces designed for human interaction;
  - Communication protocols established to enable wireless communication between devices and between devices and communications networks; and
  - Body Area Networks (BANs) or Personal Area Networks (PANs), worn on the person of the patient, that may operate in either dedicated or unlicensed spectrum bands according to FCC regulations.<sup>4</sup>

---

<sup>4</sup> These miniature short range networks represent an important aspect of mHealth technology innovation.

### 3) Network Infrastructure

- The supporting infrastructure underneath the elements of the mHealth architecture that is critical, but shared across any potential uses of mobile and wireless technology, including:
  - The Internet and its standardized protocols that enable the ability to connect devices and multiple networks together; and
  - Mobile, wireless, and fixed network infrastructure that the Internet relies on to transmit and receive data, owned and operated by large public and private network operators. These components include wireless routers, cable or digital subscriber line (DSL) modems, cellular/wireless network towers, the plain old telephone service; local area network (LAN) servers, Internet service provider (ISP) servers, data storage devices; and other devices that work in the background to enable telecommunications systems to function properly.

### 4) Software Technologies

- Programs or “apps” that aggregate, store, and analyze data collected by medical devices; and
- Programs or apps that facilitate the transmission of data through a network using standard or proprietary communications technologies.

This whitepaper frequently refers to these four elements in subsequent chapters.

**Together, Medical Device Technologies, Communications Technologies, Network Infrastructure, and Software Technologies comprise the mHealth Architecture.**

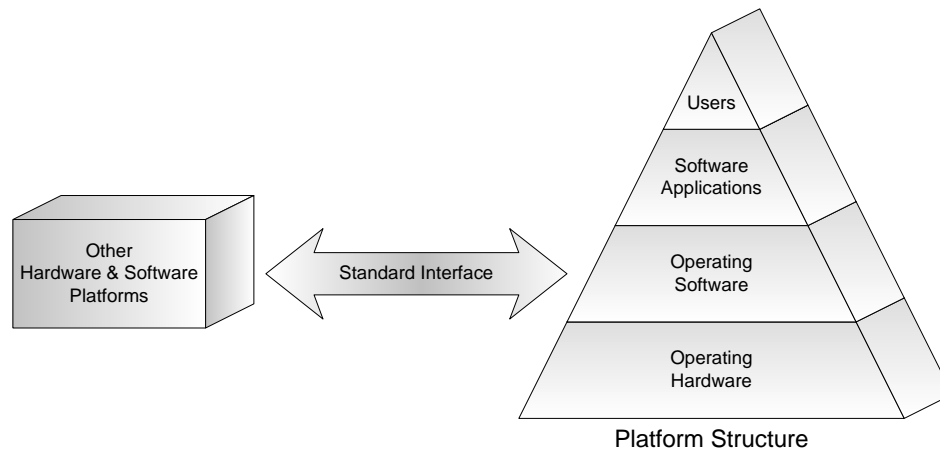
## Platforms and Interfaces

The second important concept of the mHealth definition is the idea of a *platform*. A platform is a combination of hardware and software that forms the fundamental structure on which other hardware and/or software function.<sup>5</sup> Platforms range in scope from the Internet (as a higher level platform that is accessed by familiar and standardized protocols for communication) all the way to very specific and familiar hardware devices (e.g., the iPhone) and software applications (e.g., Microsoft Windows), both of which manage direct contact with physical hardware devices and provide their own interfaces for developers and end users alike. Ultimately, a platform exists primarily through the development and adoption of software that is intended to bridge the needs and desires of developers of hardware, developers of application-specific software, and the end users of those applications and devices. Figure 1.3 provides a conceptual view of the interplay of the various elements of a platform.

---

<sup>5</sup> Some consider standard communications protocols, such as WiFi 802.11, as both a protocol and a platform, while others consider them simply as protocols. For simplicity of discussion, we will treat standard communications protocols as protocols rather than platforms.

**Figure 1.3:** A Conceptual Illustration of a Platform as a Component of an mHealth System



The PC and the Mac are examples of two platforms in the general computing realm. The PC has a specific hardware configuration that uses Microsoft Windows as its operating system. The Mac has a separate and unique hardware configuration that works in conjunction with the MacOS operating system. The PC and the Mac are distinct computer platforms that enable the use of other hardware and software. Standardization of hardware connections (e.g., USB 2.0 or Firewire) as well as standard wireless protocols (e.g., WiFi 802.11 or Bluetooth) allow peripheral hardware components to connect to both the PC and the Mac. Likewise, software developers (e.g., Adobe, who makes Acrobat and Photoshop) create applications that execute on both computing platforms. Unlike the standardization of hardware connections, software designed for these two platforms requires unique programming to function properly—that is, one version must be created for the PC and another for the Mac.

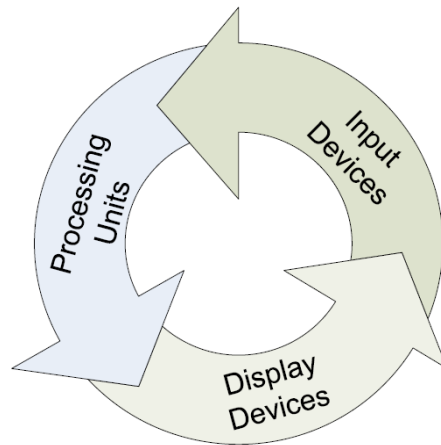
The concept of a platform already exists in the medical device industry. Pacemaker manufacturers, for example, have created unique, proprietary platforms that allow their devices to function. When a patient presents to the healthcare facility for a device checkup, the physician must use a manufacturer-specific device programmer that is designed to communicate with the patient’s device. The physician must use a separate programmer when a different patient presents to the healthcare facility with a pacemaker from another manufacturer. The software that the two programmers use are unique to the manufacturer and may even be unique to the specific device as compared to other devices made by the same manufacturer (in the same way that an old PC might use Windows XP while a new PC might use Windows 7 as its operating system).

In the new and evolving mHealth realm, the use of platforms involves connecting to one or more networks, which today generally means eventually connecting to the Internet. It is through these network connections that the value of the platform increases dramatically for mHealth technology because of the ability to access new information or new web-based software services from other sources. In the same way that software adds value to a piece of hardware by expanding the functionality of the physical device, the use of network connections and interconnecting platforms adds an additional layer of functionality. This added layer moves mHealth technology from the traditional world of isolated systems with independent platforms to a “system of systems” environment where independent platforms communicate through standard protocols.

In its simplest form, an mHealth system can be viewed from the functional perspective. That is to say that the components of an mHealth system can be viewed simply as a network of interconnecting:

- Input devices (e.g., sensors, probes, etc);
- Processing units (i.e., where analysis and algorithms run); and
- Display devices (i.e., where rendering of information occurs).

**Figure 1.4:** Functional View of a Simplified mHealth System



In this paradigm, regulatory policy might focus on the safety of certain hardware and software elements (e.g., the inherent risk of the sensor, or the output of a particular algorithm), while the communication technologies and underlying network infrastructure can be described with parameters such as the ability to reliably (i.e., within a specific probability of error) transfer information within a certain latency period.

Even from this simplistic approach, the platform concept is integral to mHealth, as it will be impossible to determine precise configurations for testing every component and other variable across the entire spectrum of mHealth. From the previous description of the architectural layers, the potential different combinations of medical devices, communications technologies, diagnostic/analytical applications, and the underlying network infrastructure are nearly infinite.

Although platforms are not a new concept, they do represent challenges for an mHealth technology regulated as a medical device, as current device requirements were developed in a time when medical use and components were much more clearly defined, identified, and easily isolated. In contrast, the power of platforms in delivering reliable functionality, consistent user interfaces, and new applications is matched only by their ability to be fluid and malleable. Moreover, the boundaries are not always clear and may change over time.

**The challenge for mHealth regulatory policy is not just embracing new technology, but new policy perspectives that account for the change from a component focus to one that is systems, platform interface, and network oriented.**

## Scope of mHealth Technology: Use Cases for FDA Regulatory Policy Consideration

Finally, our definition of mHealth has the following limits of scope:

### *Within Scope*

- Ambulatory care, ongoing chronic disease care, and monitoring of discharged patients;
- Mobile connectivity, home Internet gateways, and broadband connectivity provided by non-care facilities through access points;
- Devices connected to handsets, networks, and back-end software and data storage via the Internet (i.e., “cloud” computing, if specifically used to support mHealth applications);
- Connectivity to provider electronic health records (EHRs), electronic medical records (EMRs), and personal health records (PHRs) as destinations for data generated by mHealth;
- Licensed and unlicensed spectrum;
- Sensors, BANs, PANs, and machine-to-machine (M2M) connectivity; and
- Functional architecture between mHealth components and/or nodes on the network.

### *Out of Scope*

- Wireless systems intended primarily for use within acute care facilities such as RTLS, RFID, distributed antenna systems (DAS);
- Medical device networking, connectivity, and interoperability requirements inside an acute care facility, which are significantly different than remotely connected devices;
- Interoperability between EHR systems; and
- Technology standards selection or preference (e.g., CDMA/UMTS vs. LTE vs. WiMAX, HTML5 vs. Flash, etc).

**Our working definition of mHealth is intended to enable industry and the agency to focus on a manageable scope aligned with the overall intended use of mHealth technology—to extend the boundary of care delivery beyond the four walls of a provider’s facility through existing mobile and wireless networked technologies.**

## Conclusion

The rapid development of mHealth technologies and the diversity of the underlying components that comprise this evolving industry present a number of significant pre- and post-market questions regarding the role of the FDA in regulating this space. To promote clarity and consistency throughout this whitepaper and our future discussions with the FDA, we present a definition of mHealth and describe what is within the scope of this discussion. Specifically, we form our definition of *mHealth* around four key elements: Medical Device Technologies; Communications Technologies; Network Infrastructure; and Software Technologies.

In the chapters to follow, we elaborate on these four key elements and present the uncertainties that mHealth technologies face in light of the current legal and regulatory framework for medical devices. Our purpose is to detail the nuances of the issue and the importance of developing a guidance document specific to mHealth technology. In this way, the mHealth Regulatory Coalition intends to support the Agency's efforts to develop the appropriate guidance document that enables the FDA to fulfill its legal duty to protect and promote the public health.

## Chapter 2

### The Role of Intended Uses in mHealth Regulation

The “intended use” of a product is a key factor in determining whether the product is subject to FDA regulation as a medical device. Under the Food, Drug, and Cosmetic Act (the “Act”),<sup>8</sup> for a product to be a medical device it must be intended for a medical purpose (e.g., diagnosing or treating a disease or health condition). This chapter focuses on the particular challenges that FDA regulators, and the (potentially) regulated industry, face in evaluating the intended uses for mHealth products.

#### Background: Connecting Daily Activities, Wellness, and Disease Through mHealth

Often, even regulatory experts have trouble determining the intended uses of mHealth products when the product is intended for use in achieving a wellness outcome. Products for wellness are not regulated as medical devices, but it can be difficult to distinguish wellness from medical purposes. For example, a wellness product that assists in weight management (which is intended to promote general health) might be hard to distinguish from a medical device that is intended to treat obesity (which might serve the same general function, but is intended to treat a specific health condition).

Further complicating matters, mHealth products marketed by several different entities often are merged together in many different ways by different manufacturers or by consumers, for a variety of uses. The facts surrounding these interconnected uses can be complex and also play a crucial role in defining a given product’s intended use.

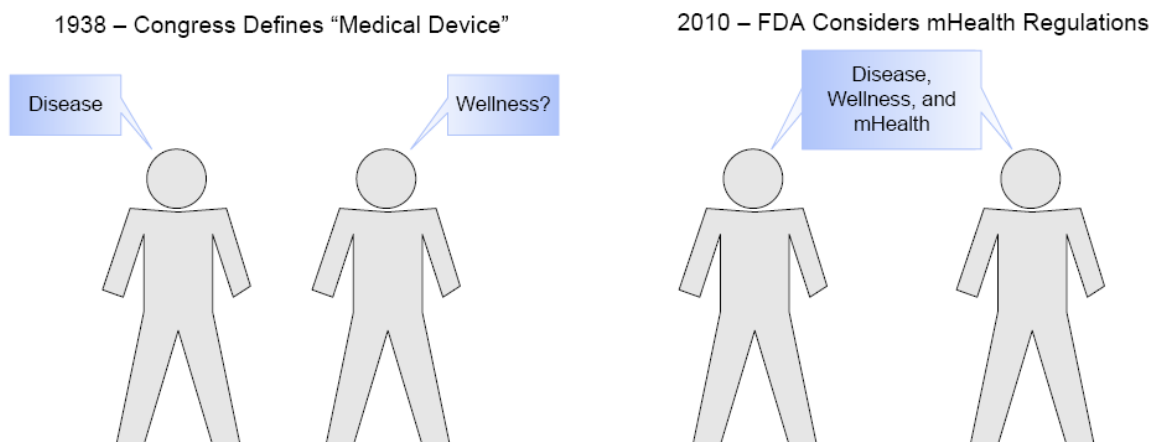
Congress could not have reasonably contemplated these issues when it first defined *medical devices* in 1938. At that time, mHealth applications were the stuff of science fiction, not real life. The understanding of the interrelationship among daily living, wellness, and disease was not as well developed, if at all, as it is today. However, Congress did have the foresight to give the FDA authority that allows it to respond to new technologies and new challenges, within the scope of the Act, in a way that serves public health.<sup>9</sup>

---

<sup>8</sup> 21 U.S.C. §§ 301–399a.

<sup>9</sup> See *United States v. Article of Drug Bacto-Unidisk*, 394 U.S. 784 (1969).

**Figure 2.1:** Then and Now: Disease, Wellness, and mHealth



The task ahead of us is not unlike the task the Agency faced when dietary supplements became popular. Prior to that, medical science did not have a sophisticated understanding of all of the connections between diet and health. As new dietary supplements were identified that improved overall health, there was also much discussion about their impact on specific diseases or conditions. For instance, the FDA had to grapple with the question of when a dietary supplement might, because of claims made, meet the definition of a drug. Ultimately, in that instance, Congress amended the Agency's statutory framework to allow citizens to make better and more informed use of dietary supplements to improve their health. Fortunately, in the mHealth area, we are not at the point where there is a need to modify the statutes because the FDA already has within its discretion the ability to draw appropriate lines of distinction.

## Legal Framework: Intended Use

Under the Act, a product meets the statutory definition of a medical device, and thus becomes subject to FDA regulation, if it is:

[A]n instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is . . . [either] *intended for use* in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals . . . [or] *intended to affect* the structure or any function of the body of man or other animals [i.e., "medical purposes"].<sup>10</sup>

The intended uses referred to in the Act are those intended by the "persons legally responsible for the labeling of devices" (for simplicity we refer to these persons as "manufacturers," although in reality the "legally responsible" person might not be the same as who actually manufactured the product).<sup>11</sup> Furthermore, those intended uses are evidenced by representations accompanying, and circumstances

<sup>10</sup> Food, Drug, and Cosmetic Act § 201(h) (emphasis added).

<sup>11</sup> FDA Device Labeling Guidance #G91-1, Mar. 8, 1991, available at <http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm081368.htm>.

surrounding, a product's distribution.<sup>12</sup> For example, a claim in a product's labeling, representation in advertising, or statement made by a sales representative could serve as evidence of intent.<sup>13</sup> Awareness that the product is being used for a purpose for which it is not labeled or advertised also could provide evidence of intended use.<sup>14</sup> Even the intent of a product's consumers might be used in evaluating the intended use of the product manufacturer.<sup>15</sup> Table 2.1 summarizes these sources of evidence of intended use.

**Table 2.1:** Sources of Evidence Considered in Evaluating a Product's Intended Use

<ul style="list-style-type: none"><li>• Product labels and labeling</li><li>• Promotional labeling and advertising</li><li>• Statements by the company, including those made by sales representatives, other employees, or paid consultants</li><li>• Uses by other manufacturers or end consumers (with awareness of the manufacturer)</li><li>• Any other evidence that bears on the objective intent of the manufacturer</li></ul>
---

Through rulemakings, guidance documents, product jurisdiction decisions, market clearances, and approvals, the FDA has given examples of various boundaries regarding intended use that, when crossed, make a product a medical device. Table 2.2 summarizes several examples.

A product that meets the legal definition of a medical device based on its intended use is subject to certain regulatory oversight by the FDA. The Agency employs a risk stratification system to categorize each medical device into Class I, II, or III—increased inherent risk of the product results in increased regulatory burden. Class III devices are subject to the highest level of scrutiny and require the greatest amount of evidence of safety and effectiveness to obtain market approval.

Although the examples in Table 2.2 provide some measure of guidance, the landscape of mHealth products and their associated intended uses reach far beyond the guidance that exists today. In the next section we illustrate challenges related to intended uses of mHealth products by posing some key questions and discussing realistic examples of mHealth technologies in use.

---

<sup>12</sup> 21 C.F.R. § 801.4.

<sup>13</sup> *Id.*

<sup>14</sup> *Id.*; *United States v. Kasz Enters., Inc.*, 855 F. Supp. 534, 539 (D.R.I. 1994).

<sup>15</sup> *United States v. Travia*, 180 F. Supp. 2d 115, 119 (D.D.C. 2001) (citing *Action on Smoking and Health v. Harris*, 655 F.2d 236, 239 (D.C. Cir. 1980)).

**Table 2.2:** Various Declarations of Intended Use that Affect Application of Medical Device Regulations in mHealth

Product	Medical Device	<u>Not</u> a Medical Device
Software	<ul style="list-style-type: none"> <li>Intended to collect data <i>directly</i> from a medical device.<sup>16</sup></li> </ul>	<ul style="list-style-type: none"> <li>Intended to allow a person to enter data manually into a computer (i.e., a person is intervening in the process, taking the data and recording it).<sup>17</sup></li> </ul>
	<ul style="list-style-type: none"> <li>Intended to store, retrieve, and display individual patient data that is collected by means other than manual entry.<sup>18</sup></li> </ul>	<ul style="list-style-type: none"> <li>Intended to perform library-type functions with information that is <i>not</i> patient-specific.<sup>19</sup></li> </ul>
	<ul style="list-style-type: none"> <li>Intended to assist in the remote administration of medication.<sup>20</sup></li> <li>Intended to analyze laboratory results and other data to provide suggestions regarding courses of treatment.<sup>21</sup></li> <li>Intended to “allow[] pathologists to view and analyze . . . slides from any computer via the internet [to] assist . . . in pathological diagnosis and prognosis.”<sup>22</sup></li> </ul>	<ul style="list-style-type: none"> <li>Intended to perform analysis of information, or provide advice regarding, a wellness purpose.<sup>23</sup></li> </ul>
Connectors	<ul style="list-style-type: none"> <li>Intended to “facilitate[] the connection between various [medical devices].”<sup>24</sup></li> </ul>	<ul style="list-style-type: none"> <li>Intended to act as “infrastructure”, allowing the exchange of information and communication between medical devices (e.g., as telephone lines, LANs, and broadband connections).<sup>25</sup></li> </ul>
Exercise Equipment	<ul style="list-style-type: none"> <li>Intended to “redevelop muscles or restore motion to joints” or for “use as an adjunct to treatment for obesity.”<sup>26</sup></li> </ul>	<ul style="list-style-type: none"> <li>Intended for “general physical conditioning” or “the development of athletic abilities in individuals who lack physical impairment.”<sup>27</sup></li> </ul>
Relaxation Equipment	<ul style="list-style-type: none"> <li>Intended for relaxation, but accompanied by claims of “other more specific medical or health-related indications for use” (e.g., a product “intended for use as a relaxation treatment for the reduction of stress . . . as an adjunctive treatment for high blood pressure”).<sup>28</sup></li> </ul>	<ul style="list-style-type: none"> <li>Intended for “relaxation” only.<sup>29</sup></li> </ul>

<sup>16</sup> Proposed Rule: Devices: General Hospital and Personal Use Devices; Reclassification of Medical Device Data System, 73 Fed. Reg. 7498 (Feb. 8, 2008).

<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

<sup>19</sup> *Id.* An example is software that allows for indexing and other library-like functions to handle general medical information (e.g., indexing the Physician’s Desk Reference).

<sup>20</sup> 21 C.F.R. § 880.6315.

<sup>21</sup> FDA Warning Letter to Patrick Rambaud, President and CEO, Seryx, Inc., Feb. 22, 2007, *available at* <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2007/ucm076282.htm>.

<sup>22</sup> FDA Warning Letter to Mohan Uttarwar, President, Biologene, Inc., May 25, 2005, *available at* <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2005/ucm075422.htm>.

<sup>23</sup> This has not been stated as such by FDA, but it seems to flow from the Act and its interpretation that wellness is not a medical purpose.

<sup>24</sup> FDA Warning Letter to Thomas R. Tribou, President, TZ Medical, Inc., Feb. 2, 2006, *available at* <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2006/ucm075787.htm>.

<sup>25</sup> Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, 18 (May 2005).

<sup>26</sup> FDA Guidance Document for the Preparation of Premarket Notification [510(k)] Applications for Exercise Equipment, 5 (July 1995).

<sup>27</sup> *Id.*

<sup>28</sup> *Id.*; K020399, Resparate Biofeedback Device (Cleared 7/2/2002); 21 C.F.R. § 882.5050.

<sup>29</sup> United States v. One Labeled Unit, 885 F. Supp. 1025 (E.D. Ohio 1995).

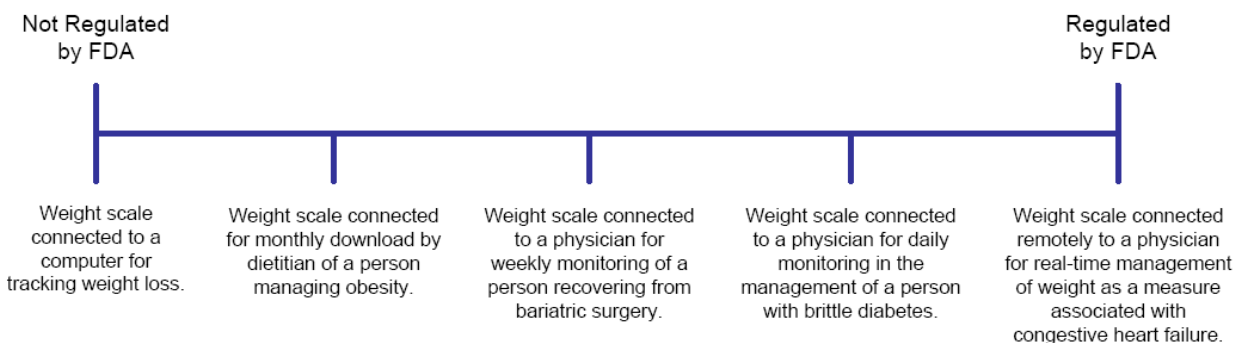
## Challenges: Evaluating Intended Use in mHealth

As explained above, the central challenge in evaluating the intended use of mHealth products often arises from the way the uses of many products are deeply intertwined with *wellness*, which can be difficult to distinguish from a *medical* purpose. For example:

- The overarching question is at what point does a product cease serving a wellness function and start serving a medical purpose?
  - When does a weight management product cross the line from assisting in health conditioning to preventing or treating obesity?
  - If the dividing line used to distinguish products is based around impairment (as with exercise equipment), how is impairment defined? In the case of weight management, would the clinical definition of obesity be used, or something else?
- To what extent, and in what ways, can a manufacturer manage the scope of intended use to “wellness” through their stated claims, promotional materials, and marketing approaches?
- To what extent can manufacturers discuss the natural implications of wellness, such as reduced risks of heart disease or diabetes, without creating a medical device claim?

The difficulty in distinguishing between wellness and medical purposes is demonstrated most clearly by looking at a product that potentially serves both purposes. A weight scale, for example, may have dual wellness and medical purpose uses. How should such products be addressed? Figure 2.2 illustrates a spectrum of intended uses for a weight scale, demonstrating the grey area between regulated and unregulated products. Somewhere along the continuum, the weight scale goes from being unregulated to regulated by the FDA.

**Figure 2.2:** Spectrum of Intended Uses for a Weight Scale



Another challenge arises from the interconnected nature of mHealth products. Given the broad scope of evidence that can define the intended use of a product, and because use of a product can change once it has left the manufacturer's control, defining intended use can be difficult. For example, would a smartphone be considered a medical device if:

- The smartphone's manufacturer also sells medical device software to run on the phone?
- A third-party medical device software app is sold through the smartphone manufacturer's online app store?
- A third-party software developer creates a medical device app that is sold directly by the third party, without involvement of, but with the knowledge of, the phone manufacturer?
- A third-party software developer creates a medical device app that is sold directly by the third party, without the knowledge of the phone manufacturer?

The above are some of the broader questions. However, to illustrate in greater detail the potential challenges that mHealth products could face with respect to intended uses, the following real-life, fact-based scenarios demonstrate the shifting of intended use of multiple mobile technologies associated with a weight scale. For each scenario, we offer specific questions that might be raised regarding the intended use. The components common to each scenario below are:

- A digital weight scale;
- Wireless transmission of weight results for transmission via Bluetooth connectivity;
- A smartphone connected to a 3G network;
- Software to capture and transmit the results data; and
- An algorithm to trend the weight data.

In each of the scenarios, unless otherwise noted, we assume that the manufacturers promote the given use case through its advertising and other materials. In addition, consistent with the statutory requirements for medical device regulation mentioned above, the intended uses presented below are that of the *manufacturer*, rather than the intended use of the *end user*. This is an important point. The law makes it clear that intended use is determined with reference "to the objective intent of the persons legally responsible for the labeling of devices."<sup>30</sup>

## Scenario 1: Consumer Weight Management

*A manufacturer sells the mHealth system to an overweight consumer for general fitness and health improvement purposes (i.e., to lose weight). The consumer steps on the scale each day and captures his current weight. The weight measurement is transmitted via wireless connections to the consumer's mobile smartphone, which has a software app that records the data and sends it to a PHR hosted via the Internet. The app on the smartphone also trends the data and provides the consumer with a daily progress report based on the previous day's recording, indicating whether or not the consumer's weight*

---

<sup>30</sup> 21 C.F.R. § 801.4

*has increased or decreased. The consumer's PHR software stores all of the daily readings and provides the ability to look at the consumer's weight over a given time period.*

This scenario poses a number of challenging questions, including:

- To what extent can the manufacturers of the components discuss the potential benefits of weight management to overall health (e.g., reducing the risk of certain health conditions) without suggesting the product is intended for a medical purpose?
- Assume the weight scale was sold separately from the other products, and intended for a medical purpose by its manufacturer (i.e., it was a stand-on scale classified under 21 C.F.R. § 880.2700).<sup>31</sup>
  - If the data collection and management products used in the above scenario were compatible with a medical device scale, and the products' manufacturers knew of the compatibility, would this be evidence of a medical purpose intended use?
  - Does the answer change if the original design was not compatible but subsequently the user is able to download a driver that enables compatibility? Does it depend on who supplies the driver or whether the manufacturers of the other products are aware of the driver's availability?
- What steps, if any, must manufacturers take if they want to ensure a product's intended uses do not grow beyond the scope of wellness?
  - Mere off-label use of a product is not sufficient to change the nature of the product from a wellness to medical purpose. In light of that, does the FDA agree there are no specific design features or labeling that the manufacturer must use to restrict the use of the product to wellness purposes?
- What influence does the PHR component have on the overall intended use? Does the manufacturer's intended use become more *medical* if the weight measurements are sent to a PHR hosted by the consumer's health insurer or health management organization as opposed to an independent Internet site?
- To what extent does the content of the daily progress report and the periodic data trending evidence a *medical* intended use?

## **Scenario 2: Bariatric Surgery Patient**

*A consumer elects to undergo bariatric surgery to address his weight problem that has now become more serious. The manufacturer sells an mHealth system that allows the patient and his physician to track the patient's post-operative progress through daily weight measurements and to determine the success of the procedure. The smartphone app remains responsible for receiving and transmitting data from the wireless weight scale to a PHR maintained by the patient. The smartphone app now has the additional responsibility of forwarding the results to the patient's primary care physician's EHR system.*

---

<sup>31</sup> As discussed in the legal foundation of this chapter, products (e.g., software) that are intended to collect, transmit, and store medical data can themselves be medical devices.

*This is the same physician who referred the patient to the bariatric center that performed the procedure. The primary care physician's EHR system has the ability to share the results with the bariatric surgeon via either a web portal view, or through transmission of the results. The smartphone app functionality remains the same—allowing a comparison of results on a daily basis—with the forwarding of each daily reading to the EHR systems as described.*

*A new app is developed and downloaded to the patient's smartphone. This new app has the ability to run an algorithm on the phone that trends the data according to set parameters, which trigger a notification to the patient's primary care physician should unusually fast weight loss occur. The parameters are defined by the physician and then the app is downloaded onto the smartphone from the handset manufacturer's app store. The app only works with the previous release of the handset software. As a result, the patient cannot upgrade the phone to the latest version of the smartphone operating system.*

- The app in this scenario is developed for use by a physician for a medical purpose. Is its medical use, alone, sufficient to evidence the manufacturer's intended use?
  - What if the particular app function, which allows trending and notification, was actually intended by the manufacturer for a wellness purpose, as part of an overall health conditioning regimen (with the notification being directed to a physician, trainer, or other individual or automated system that is helping to guide conditioning)?
- Does the ability of the app to notify a physician about weight loss based on physician-defined parameters indicate that the product is a medical device?
- Would it matter if the app was promoted exclusively as an aid to help consumers manage weight as part of overall wellness with guidance from a physician or other individual, as opposed to post-operative monitoring?
- Would the fact that the app is being used for post-operative monitoring be sufficient evidence of the app manufacturer's intent to make the product a medical device?
- Assuming the app is considered a device, is selling the app through the smartphone manufacturer's app store evidence that the smartphone is intended for a medical purpose? Does the evidence of intended use change if the app is downloaded from a third party or if a third party develops the app, but the smartphone manufacturer or the wireless network carrier sells the app in its app store?
- Does the physician's ability to provide feedback or a recommendation based on the measured data demonstrate intended use? Does the intended use change if the feedback is provided via a phone call as opposed to sending a recommendation to the patient's device?

*The manufacturer markets an upgraded system that allows multiple medical devices, including the weight scale, to communicate to the smartphone. Because the patient also suffers from mild hypertension and elevated blood sugar levels due to a pre-diabetic condition, the physician recommends that the patient use a blood pressure cuff and a glucometer to track improvements in blood pressure and blood sugar levels. The three devices transmit their data wirelessly to the smartphone weight management app, which now transmits three measurements to both the patient's PHR and the physician's EHR. The algorithm of the smartphone was designed only for weight measurement; therefore, the other two data sources are sent in raw, unmodified formats to the EHR system. The EHR*

*system contains software that is capable of trending the blood pressure and blood sugar data, combining those results with the data reported from the smartphone app, and consolidating them into a single report that tracks overall patient progression or regression, with alert triggers to notify the physician if the condition is serious enough to warrant notification.*

The smartphone app's ability to collect and transmit data from products that were clearly intended to be medical devices would seem to make the app a medical device, as discussed in Table 2.2. However, a number of relevant questions remain, including:

- Does designing the smartphone in a way that allows the collection and transmission of blood pressure cuff and glucometer medical device data make the phone a medical device?
- Would the ability to create a link between the medical devices and an EHR system, with its trending and notification software, make the app or the smartphone a medical device? Does the answer change if the app/smartphone used standard technology that any number of medical and non-medical devices could use to facilitate data transmission?
- What impact does the app or smartphone manufacturers' awareness of these uses have on the determination of intended uses? What if their respective manufacturers did not promote these kinds of uses? What if they specifically disclaimed these kinds of uses?
- Could the wireless network carrier promote features of their network (e.g., coverage stability, reliability, or quality of service delivery) in the context of health data transmission and still be considered "infrastructure" that is not subject to medical device regulation?

*The manufacturer also markets a system that simply records patient parameters and allows the physician to access the data for general continuity of care. Because the surgery has been deemed successful and the patient's blood pressure and blood sugar readings are no longer in elevated states that would require daily monitoring, the physician informs the patient that it is no longer necessary to use the physician's EHR system. However, the doctor encourages the patient to maintain a healthy diet and exercise regimen and to weigh himself daily. The patient uploads the information to his PHR, which has the ability to share the results with the physician as a continuity of care record (CCR). The patient asks the doctor if it would be useful to have access for the annual checkup. The doctor responds affirmatively.*

- Does the patient's PHR system, which allows data sharing not specifically for a medical purpose (e.g., sharing the data with fellow dieters for support), have a different intended use if it can also be used with a CCR?
- How would the PHR or smartphone manufacturers' awareness of these uses affect the determination of intended uses for their respective product? What if the manufacturers did not promote these kinds of uses? What if they specifically disclaimed the uses?

### **Scenario 3: Cardiac Care Patient**

*Unfortunately over time, the consumer begins to notice that during the normal course of his exercise routine he feels very faint and light headed, even to the point of losing consciousness. Upon examination by his physician, the consumer is diagnosed with tachycardia, an abnormally fast and irregular heartbeat. The patient's healthcare provider determines that the individual would benefit from an implantable cardioverter defibrillator (ICD), requiring one to two days in the hospital to have the device*

*implanted and to conduct testing of its operation. The operation is performed and the patient is discharged from the hospital with instructions and assistance in setting up a remote monitoring system for the ICD and some associated care devices that include a blood pressure cuff, a weight scale, and a new wireless pulse oximeter.*

*The manufacturer of the remote monitoring system installed in the patient's home also markets a smartphone app that collects and transmits the ICD data through a wireless connection while the patient performs his normal daily activities. The data are sent directly to the central monitoring system operated by the ICD device manufacturer for subsequent analysis and sharing with the patient's physician, including transmission to the physician's EHR system. The data from the blood pressure cuff, weight scale, and pulse oximeter can be transmitted with the ICD data through the mobile phone's wireless connection. These data are synched with the patient's in-home remote monitoring device to ensure reliability and accuracy. Due to the complexity of the data and the analysis needed to be conducted, the ICD manufacturer has developed a clinical analytics and decision support software application that makes predictive assessments of the patient's condition. If threshold limits are exceeded, the analysis software notifies the cardiologist and/or primary care physician as necessary. SMS text messages can also be sent to the patient's phone to alert them of the results of the analysis conducted by the clinical decision reporting system. Results of the patient's monitoring measurements can be posted into the patient's PHR directly from the smartphone, but the ICD remote monitoring system is responsible for updating the primary care physician's and cardiologist's EHR systems. It is also available for viewing through a portal with log-in access permissions.*

- Does the ability of an existing peripheral device (e.g., weight scale, blood pressure cuff, or pulse oximeter, etc.) to connect to the remote monitoring system evidence the intended use of the peripheral device manufacturer?
  - Does the answer depend on whether the peripheral device uses standard communications protocols?
  - What if the manufacturer specifically disclaims such use?
- Does the ability of the smartphone or smartphone app to transmit data from the remote patient monitoring system to the ICD manufacturer's central monitoring system evidence a *medical* intended use?

## Conclusion

The scenarios presented in this chapter highlight the challenges that manufacturers face when marketing the various components of an mHealth system. Although these scenarios centered around the use of a weight scale, they represent questions that apply generally across the spectrum of mHealth systems. The intended use of a particular component may vary depending on the complexity of the system and the design features of that component. The grey area between wellness and medical purpose creates significant uncertainty as to whether a given product in a given situation will be deemed to have the intended use that implicates medical device regulation.

In the next chapter, we discuss the implications of medical device regulation on the hardware components and their connections within an mHealth system.

## Chapter 3

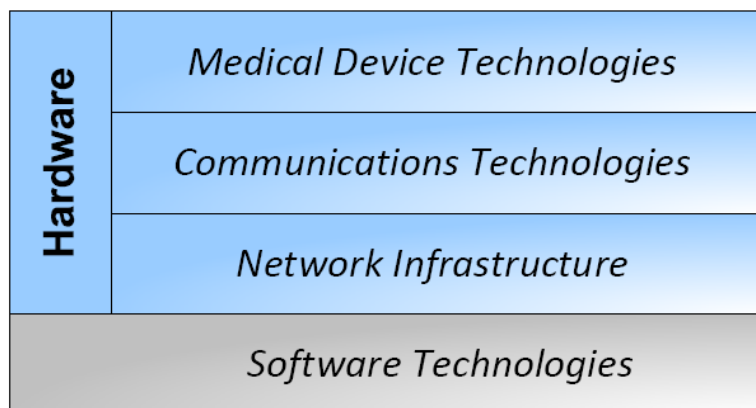
# Connections Between Hardware: The “Accessory Rule” and mHealth

Connections between hardware are what puts the “mobile” in *mobileHealth* (mHealth), and are what drives much of the potential value mHealth technologies offer. The potential benefits to patients from these kinds of connections range from quality of life—letting patients live their life less impeded by doctor’s visits, stays in care facilities, and the like—to detecting life-threatening conditions in time to prevent serious harm to patients. If integrated into our health care system, these connections also could pay enormous dividends to the public in terms of cost savings and efficiencies in care. As explained in Chapter 1, the FDA’s regulation of these products is going to be a major factor in determining how the growth and benefits of these technologies play out.

In Chapter 2 we tackled the issue of intended uses, including how a product’s uses determine whether the product is a device. In this chapter we delve into how connections between and among hardware products in mHealth impact their FDA regulatory status. Here, the central regulatory question is whether a product is considered an “accessory” to another medical device, a stand-alone device that simply happens to talk to other devices, or something that plays a role in making an mHealth system work but is not regulated as a device at all.

The discussion in this chapter demonstrates the need for clarity regarding the regulation of mHealth technologies. **If we applied the accessory rule as it is currently understood, the impact could be huge and overly burdensome for the public, the FDA, and the future of mHealth technology.** In thinking about these issues, it is helpful to use the conceptual framework of the four key elements of an mHealth system that we laid out in Chapter 1 of this whitepaper. Figure 3.1 illustrates this framework.

**Figure 3.1:** The Four Key Elements of an mHealth System

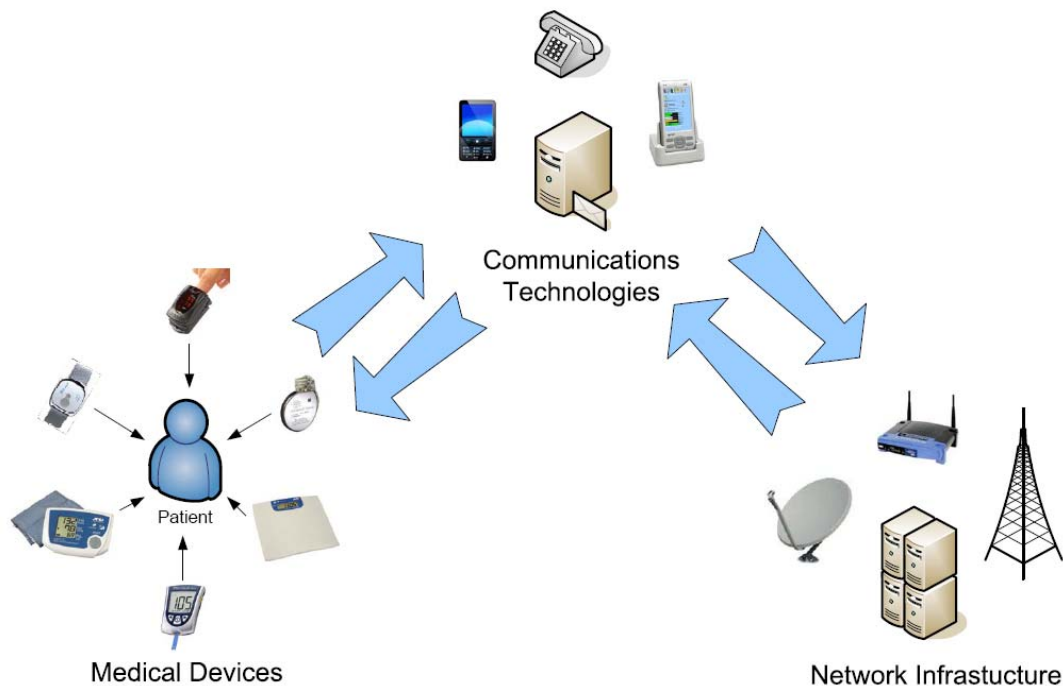


Because we are talking about hardware here, and because software has its own special place in mHealth, this chapter focuses on connections between and among products in the **first three categories** of this framework and leaves software for Chapter 4. We also will consider the impact and role of an



Now let's hone in on the three hardware elements of our four-prong conceptual framework—Medical Device Technologies, Communications Technologies, and Network Infrastructure. As illustrated by Figure 3.2, each of these three key elements is an essential part of the overall scheme of this mHealth system. Each hardware component acts as a transmitter and processor of information, and each raises various regulatory issues via its connections to the others.<sup>32</sup> Figure 3.3 shows examples of the pieces of hardware that commonly form the basis of mHealth technologies and their respective element of the conceptual framework. Intertwined with all this is a human component—i.e., the connections mHealth technologies make between a patient and the healthcare provider.

**Figure 3.3:** Examples of Connected Hardware Components of an mHealth System



Below, we go through each of these elements in turn, diving into their definitions and explaining the connections that make the FDA “accessory rule” a conundrum.

### *Medical Device Technologies*

For this whitepaper, medical device hardware includes products that are intended to diagnose and treat disease or other health conditions. These range from the very simple, like a weight scale, to the very complex, like ambulatory cardiac arrhythmia sensors or an implantable pacemaker.

---

<sup>32</sup> Although software can be described as transmitting and processing information as part of an mHealth technology, this discussion is limited to the *physical* rather than *virtual* transmission and processing of information.

With the advent of wireless telecommunications, many of these medical devices have evolved from an independent and stand-alone existence into a complex network of machines that “talk” to each other, transmitting data between devices, where before those data would have been collected and stored by a contained unit. Here are some examples of what we mean by *Medical Device Hardware*, along with some of the drivers behind integrating this element into mHealth systems:

- Mobile cardiac outpatient telemetry (MCOT) marries a standard Holter monitor (i.e., Medical Device Hardware) to a mobile phone. MCOT records a patient’s electrocardiogram (ECG) and transmits the ECG data via a wireless communications network to a healthcare professional. MCOT might lead to real-time, or close to real-time, monitoring of a patient, which could provide faster help to the patient (e.g., faster diagnosis or treatment decisions).
- CardioNet’s SomNet technology uses an enhanced MCOT system for remote patient evaluation and diagnosis of sleep apnea in the patient’s home. This technology might motivate people to get diagnosed sooner because it eliminates the hassle of going to an overnight sleep clinic. Also, what once required buildings dedicated to sleep studies could now be brought to a patient’s home, which might, in the long term, bring institutional benefits in terms of cost savings.
- The WebVMC RemoteNurse Patient Monitoring System makes use of off-the-shelf medical devices to collect blood pressure, glucose, weight, SpO<sub>2</sub>, peak flow, ECG, and other patient data, including a digital camera for visual analysis of the patient. The system uses a touch-screen display for presenting patient prompts and pre-defined questions and a hardware console to collect data from the connected medical device hardware. The system allows a healthcare provider to remotely assess patient conditions.
- Airstrip RPM is software that runs on devices capable of running Apple iPhone OS. It interfaces with third-party centralized monitoring systems that in turn gather data from patient monitors and other devices in the healthcare facility. AirStrip RPM gives healthcare providers the ability to view remotely near-real-time patient physiological data, including ECG, invasive blood pressure, non-invasive blood pressure, heart rate, pulse oximetry, and carbon dioxide.
- Boston Scientific Corporation’s Latitude Patient Management combines data from multiple medical devices—an implantable pacemaker/defibrillator, blood pressure cuff, and weight scale—to enable monitoring the ICD status and certain health parameters of the patient. This technology enables a patient to maintain his or her normal daily activities and eliminates some of the face-to-face visits with healthcare professionals that would otherwise have to occur.
- BANs and PANs use sensors on, in, or near patients to facilitate monitoring of health and wellness parameters. For example, BodyMedia’s FIT weight management system uses an armband sensor to measure physical activity and body temperature in order to calculate energy expenditure and employs a scale for recording weight loss or gain.

### *Communications Technology*

Operating in the background, but crucial to creating the links between medical devices, is communications technology. This includes the wide array of machines and equipment that interact with each other for the purpose of transmitting data from point to point and ultimately to a physician or

patient, as illustrated in Figure 3.2.<sup>33</sup> Communications technologies might be commonly thought of as *devices*, but generally they are distinct in that the machines do not directly impact patient health—communications technology hardware helps the devices talk to one another. These kinds of products include:

- A mobile phone;
- A personal computer;
- A PDA;
- A plain old telephone; and
- A proprietary communication device.

Importantly, these products do not necessarily transmit information just between two medical devices. They might transmit to several devices and/or non-devices (e.g., hardware for medical billing systems) through a chain of communication technology, or through a web that allows the information to be transmitted to multiple products simultaneously. There is a lot more than just a cable connecting two pieces of equipment.

Importantly, these data transmissions are *virtual* in that a physical manifestation of the data may not exist. The wired and wireless protocols as well as the cellular communications employ electrical impulses and radio waves to transmit the data. It is the underlying *network infrastructure* that enables these transmissions to eventually get to the device that allows the patient or doctor to see it. This brings us to our third and final hardware category.

### *Network Infrastructure*

Network infrastructure is an essential component of an mHealth hardware system. Without the physical components that establish the network, data transmission and patient diagnosis and treatment returns to the pre-Internet age where medical devices were isolated and often required direct clinician interaction to facilitate patient care. The network infrastructure is a combination of machines and equipment that generate, receive, interpret, and transmit information from the patient to the healthcare provider and every point in between.<sup>34</sup> The network infrastructure for any given mHealth system can include any combination of the following:

- A wireless router;
- A cable or DSL modem;
- A wireless or cellular tower and radio access network;

---

<sup>33</sup> In the mHealth setting, the *end user* is a patient or healthcare provider.

<sup>34</sup> Although the machines and equipment that compose the network infrastructure at the micro-level consist of electrical components and impulses, at the end user or macro-level, the fourth element of the mHealth technology—Software Technology—is integral to the realization of the data transmitted. These software applications that facilitate the end user to visualize the data should not be confused with software programs that execute machine commands to facilitate the transmission of information throughout the network infrastructure.

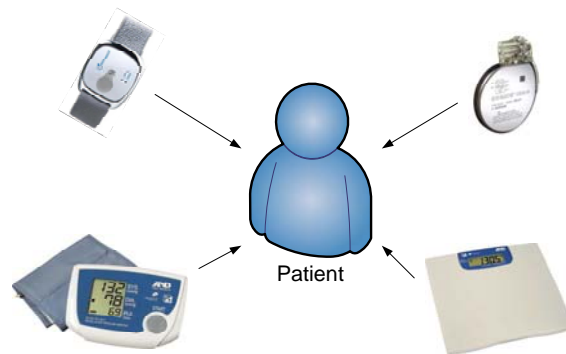
- A plain old telephone service;
- LAN servers;
- ISP servers;
- Data storage devices; and
- Other devices that work in the background to enable telecommunications systems to function properly.

In fact, it would be impossible to isolate wireless/mobile mHealth hardware completely from its wired brethren, as the mobile networks we rely on eventually connect via fiber optic cables to the Internet. Network infrastructure hardware is highly interdependent on *wired and wireless* components alike, regardless of how the end user connects to the interconnected network we call the Internet.

### *The Human Component*

The connections that mHealth technology makes between a patient or the healthcare provider play an important role in how they are regulated. As a result, understanding the human components of a given mHealth system is critical to understanding the technology itself, as well as regulatory implications. Consider, for example, a patient (shown in Figure 3.4) with an ICD, an armband sensor for measuring body temperature and physical activity, an external blood pressure cuff, and a scale for monitoring changes in body weight.<sup>35</sup>

**Figure 3.4:** Patient-Centered Connections with mHealth Technologies

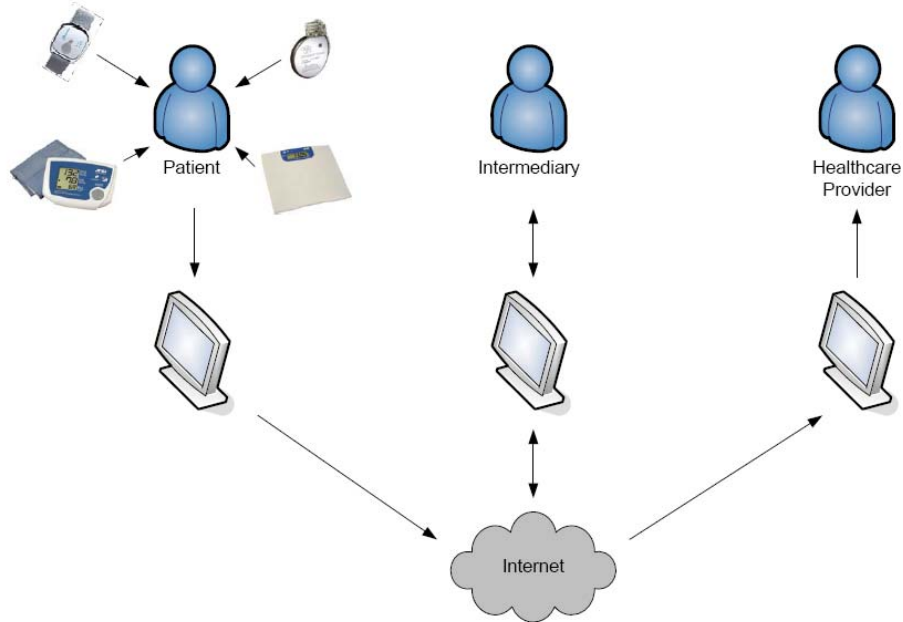


Assume none of these gadgets needs to rely on the other to function properly, yet the patient's disease management requires the use of each of the devices. The patient (or the devices themselves) may transmit the data via the Internet to a healthcare provider. Alternatively, a third-party intermediary may review the data before final transmission to the clinician, as shown in Figure 3.5.

---

<sup>35</sup> Independently, the ICD would be a Class III medical device, the armband sensor may be unregulated (depending on the intended use), the blood pressure cuff would be a Class II device, and the scale would be a Class I device (depending on the intended use). If each of these components are connected to the same patient as part of an mHealth system, the accessory rule would require that all components be regulated as a Class III medical device.

**Figure 3.5:** Simplified Diagram of a Generic mHealth System



This human component isolates those mHealth components with which the patient, intermediary reviewer (e.g., manufacturer’s clinical staff or a clinical call center), and healthcare provider directly interact. The remaining components of an mHealth system work in the background to facilitate the flow of data throughout the system. Looking at an mHealth system from this perspective—with the human at the center—may help distinguish those elements of the system that warrant regulatory oversight from the products that merely enable mHealth to exist.

\* \* \*

In summary, these elements of mHealth technologies are simply hardware that work in concert—via connections—to connect patients, health care providers, data, and care. The above discussion is important to understand where mHealth technologies are today and what the future holds for this rapidly evolving industry. The remainder of this chapter will focus on our existing legal framework and the challenges that it imposes on continued innovation.

## Legal Framework: Accessories and Components

In the mHealth area, a large number of the regulatory issues we run up against involve the relationship between two or more pieces of hardware (one or more of which is a medical device) and how the FDA defines and controls that relationship. To get started on the legal framework relevant to these issues, under the Food, Drug, and Cosmetic Act, a product that supports (i.e., is connected to) another medical device could be:

- A medical device in its own right;
- A “component” of the medical device; or
- An “accessory” of the medical device.

Components and accessories are themselves medical devices, although the regulatory requirements for each vary significantly. Understanding the definitions and regulation of both components and accessories is important for our discussion.

Starting with the definitions, an *accessory* is a finished device that is “distributed separately but intended to be attached to or used in conjunction with another finished device,” often called the *parent* device.<sup>36</sup> A *component*, on the other hand, is something that is “intended to be included as part of the finished, packaged, and labeled device.”<sup>37</sup> At bottom, the difference between an accessory and a component is who buys it—end users buy accessories to use with other finished devices, while manufacturers buy components to incorporate into a finished device. Further, the accessory/component analysis turns on evaluating the item’s intended use with the same approach described in Chapter 2, but with the focus turning to the issue of whether the item is intended to be attached or used in conjunction with another device, whether the item is sold directly to an end user, and when the marriage of the products is intended.

## How Does FDA Regulation of Components Differ from Accessories?

First, a quick, high-level refresher on medical device classification generally. The level of regulation for a medical device is usually based on the potential risks associated with the device’s intended use and its indications for use. The device’s “classification” (Class I, II, or III) identifies the level of regulatory control for the device and generally identifies the marketing process the manufacturer must complete in order to obtain FDA clearance or approval for marketing.

Components, because they are intended for incorporation into a finished device, are exempt from most FDA regulatory requirements, with the regulatory burdens being borne by the finished device manufacturer who uses the component.<sup>38</sup> In other words, components are mostly regulated as part of the finished product they are included in, so the finished device classification (once the component is incorporated in the finished product) governs the regulation of that component.

Accessories, on the other hand, because they go right to the end user, must meet the FDA requirements applicable to them before they leave the hands of the accessory manufacturer.<sup>39</sup> The obvious next question is what FDA requirements apply to accessories? The answer is not always clear. From a patchwork of FDA presentations, guidance documents, our own experience, and other materials, it seems like the following basic principles usually govern accessory regulation:

---

<sup>36</sup> CTR. FOR DEVICES & RADIOLOGICAL HEALTH, FOOD & DRUG ADMIN., HHS PUB. NO. FDA 97-4179, MEDICAL DEVICE QUALITY SYSTEMS MANUAL: A SMALL ENTITY COMPLIANCE GUIDE (Dec. 1996), *available at* <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/QualitySystemsRegulations/MedicalDeviceQualitySystemsManual/default.htm>; FDA Guidance for Industry: Blood Establishment Computer System Validation in the User’s Facility, 3 (Draft, Oct. 2007), *available at* <http://www.fda.gov/downloads/BiologicsBloodVaccines/GuidanceComplianceRegulatoryInformation/Guidances/Blood/ucm078815.pdf>.

<sup>37</sup> 21 C.F.R. § 820.3(c).

<sup>38</sup> *See, e.g., id.* §§ 807.65(a), 820.1(a), .3(c), (l).

<sup>39</sup> *See, e.g., id.* §§ 820.1(a), .3(l), .20(a)(5).

- If the product falls within its own regulatory classification, the accessory is regulated under that classification.<sup>40</sup>
- If the product does not fall within a regulatory classification, it is regulated as the parent device (this is sometimes referred to as the “accessory rule”).<sup>41</sup> So, for example, if a product—even a really simple one from a technology standpoint—becomes an accessory to a Class III device, it can become subject to very onerous regulatory requirements.
- If the product has multiple parents, it is regulated with the classification of the highest classified parent.<sup>42</sup>

These are general guidelines. We understand the FDA is currently in the process of crafting a specific policy for mHealth apps, but that is in its early stages of development. There is some existing piecemeal guidance. For example, an Agency medical device software guidance document says that communications infrastructure, such as telephone lines and broadband connections, that allows exchange and communication between medical devices will not be regulated as medical devices.<sup>43</sup> However, there has not been a comprehensive statement of how potential accessories would or would not be regulated across the mHealth industry. Just as with intended uses, getting clarity about how the FDA plans to regulate these interconnected pieces of mHealth technology is something that the mHealth industry needs to foster its continued growth. And therein lie the challenges.

## Challenges: Determining the Scope of the “Accessory Rule”

The fundamental challenge is this: Historically, the “accessory rule” has been thought of as an overarching rule, broadly applicable to nearly all parent device-“accessory device” connections. What are the boundaries in the mHealth world? In today’s rapidly developing technological landscape, the boundaries between accessories and stand-alone devices are not always clear and may lead to regulatory requirements that are incongruent with the risk level of the product being regulated. **Indeed, if the current accessory rule were applied equally across the spectrum of mobile and wireless-enabled medical devices, mobile phones, entire cellular networks operated by carriers such as AT&T and Verizon, and even the Internet itself, could potentially be considered accessories to a device.**

A number of specific ambiguities and challenges flow from that broadly stated regulatory problem statement. Let’s take the most general ones first, then work through some specific examples.

---

<sup>40</sup> Heather Rosencrans, Director, 510(k) Staff, FDA CDRH; Presentation: 510(k) Overview, *available at* <http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm126288.htm>.

<sup>41</sup> *Id.* The accessory rule is not a “rule” in the sense of an administrative rulemaking, but is merely a general policy that FDA has historically used to regulate accessories to medical devices.

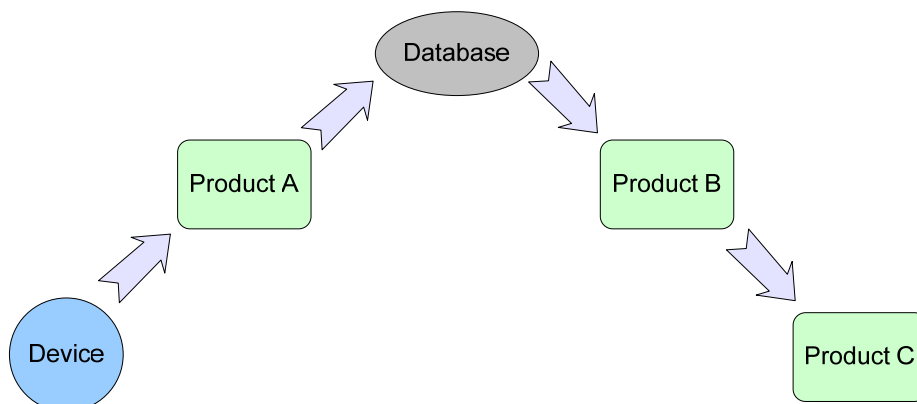
<sup>42</sup> FDA Guidance, Content of a 510(k), *available at* <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/ucm142651.htm>.

<sup>43</sup> Guidance for Industry and FDA Staff: Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, 18 (May 2005).

## General Questions

The primary general questions include:

- What happens to “accessories to accessories”? That is, in mHealth, there may be a configuration as shown in Figure 3.6, where Product A receives information from a Device, a Database (stored on Product B) receives information from Product A, and Product C receives information from Product B.
  - If the original parent Device means that Product A is a medical device, then does Product A render the Database a device?
    - If so, does the Database render Product B a device?
    - If so, does Product B render Product C a device?
    - If there is a break in this chain at any point, does that render the remainder of the products in the chain unregulated?
  - In any of these scenarios, how is the classification of each product determined? Does the accessory rule apply such that all products in the chain are classified as the classification of the Device?
  - Does the function of Product A, B, or C or the Database affect whether the component is regulated or, if regulated, its classification?
  - If Product A, for example, is a standard piece of hardware that can be interchanged with a number of other standard products (e.g., a DSL filter, a PSTN to cellular adapter, USB wireless network adapter/modem, etc.) based on the end user’s configuration needs, is the standard product considered an accessory?
    - Does the answer depend on whether the manufacturer of the Device recommends a particular piece of hardware for Product A?
    - Does it matter if the product uses a licensed or unlicensed wireless spectrum?



**Figure 3.6:** Example of Potential “Accessories” to a Medical Device and Other “Accessories” in mHealth

- For specific kinds of products, the FDA has suggested that some hardware components are not regulated (e.g., network infrastructure).<sup>44</sup> Is this rule generally applicable to mHealth products? How do companies know when to apply it?
  - Does uploading firmware to a medical device via a public, wireless network affect regulation of the network infrastructure?
  - Is a wireless network regulated as an accessory if a medical device is embedded with a chip that enables the device to transmit data via that network directly, as opposed to transmitting the data to an intermediary product (e.g., a computer or smartphone)?
  - Does the transmission mechanism (i.e., store and forward vs. real-time) affect the regulation of the wireless network? Do the regulatory requirements change if the transmission function is part of a software app as opposed to part of the transport hardware?
- In what circumstances does an existing regulatory classification for a potential accessory override the accessory rule?
  - To take the example in Figure 3.6, what if the Device is Class III? Under the current accessory rule, Product A would be regulated as a Class III device. But if Product A is independently a Class I or II medical device under an applicable classification regulation, does the independent classification of Product A predominate such that the accessory rule does not apply?
  - Does the answer depend on intended use of Product A?
  - Does the answer depend on inherent risk of the combination of Product A with the Device?
- Sometimes whether an accessory could fall within an existing classification is not so clear, and considerable judgment needs to be exercised, particularly for Class I exempt devices that would not be submitted to the FDA. How do companies navigate these gray areas? Can companies use the *de novo* classification process for low risk devices?
- Who is responsible for reporting adverse events and for submitting post-market modification applications when a system component is updated?

The examples below further illustrate the complexity of these questions.

### Example 1: A Weight Scale as Part of an mHealth System

This hypothetical product has the following system components:

- A **weight scale** to detect changes in body mass due to heart failure decompensation;

---

<sup>44</sup> *Id.*

- A **blood pressure cuff** to measure changes in blood pressure associated with changes in heart failure condition;
- An **ICD** for the detection and treatment of heart failure;
- A **proprietary communication device** that collects and transmits data from each of these components to a proprietary database located on a proprietary server network;
- Various **database access devices** (e.g., computer or smartphone) for:
  - Review of patient data by a trained clinical staff within the manufacturer's proprietary network;
  - Evaluation of patient data for billing or customer service purposes;
  - Analysis of patient data for alert notification;
  - Analysis of patient data for research and development purposes;
- A **web application server** for hosting a website that allows a healthcare provider to access the patient data; and
- A **web application access device** (e.g., computer or smartphone) for allowing a healthcare provider to access the patient data, to program alert notification settings, and/or to control device functions.

The configuration of the products above raises several questions. Even just focusing on a plain old weight scale gives a good feel for the complexity of the issues:

- Is the incredibly low risk weight scale regulated by the existing classification<sup>45</sup> for such sensors? Or does its direct connection with the ICD render that weight scale a Class III device, as an accessory to the ICD? Does the weight scale even fall within the accessory rule at all?
- If a device receives information from the weight scale through one or more intermediary products (e.g., a computer or smartphone), do the intermediary products shield the scale from becoming an accessory to the medical device?
  - Are the intermediary products regulated in the same classification as the parent device? If so, does that classification apply to all products in the chain (i.e., the weight scale)?
  - Would the highest classification in the chain be imputed to all the products in the chain, including those products that would otherwise not be classified as a medical device (e.g., a computer or smartphone)?
- How would the answers to the question above change if instead of going through a chain, the products were connected through a web, with the sensor transmitting to multiple products?

---

<sup>45</sup> 21 C.F.R. § 880.2700.

- For example, instead of the weight scale sending information to a single device, the scale could also send information to a computer, a smartphone, a tablet, a web server, or any number of products that are interconnected. Do the interconnections of these products affect the regulatory classification that applies to the sensor or any other product in the web of connections?
- To what extent is the weight scale manufacturer required to ensure the proper functionality of potential accessories and the underlying network infrastructure for each of the products in the web? For instance, if a smartphone has multiple modes of data transmission, is the smartphone an accessory such that the weight scale manufacturer must ensure proper data transmission in all possible modes of the smartphone?
- How would human intervention at some point in the process affect the application of the accessory rule, and the resulting classification?
  - For example, if the weight scale transmits data to a computer and the computer requires the patient to actively send the information (e.g., via email or the click of a button) to a healthcare provider, does this human interaction affect the relationship between the scale and the computer?
  - How do the regulatory requirements change if the human interaction is not the patient but is a trained clinician (e.g., physician, nurse, or physician assistant employed by the manufacturer) other than the patient's healthcare provider?
- To what extent does the answer to the questions above change if the information flows bi-directionally (i.e., both from the patient/device to the healthcare provider and from the healthcare provider to the patient/device)?

## **Example 2: A Smartphone as Part of an mHealth System**

Now consider a smartphone that is used to transmit data from a medical device connected to a patient to the physician for review. (By way of illustration, recent advertisements for the iPhone 4 have shown medical applications as one of its capabilities.)

The following questions remain unanswered:

- Is the smartphone an accessory to the medical device if the phone manufacturer promotes or intends for the phone to be used as part of an mHealth system by the patient or physician?
- Is the test for determining application of the accessory rule a "one purpose" test such that if any one purpose for using the smartphone has a medical device application then the manufacturer must comply with FDA regulatory requirements? Would this require manufacturers of smartphones to design separate models of the phones—ones that work with medical products, and ones that prohibit use with medical devices?

To illustrate the complications with respect to adverse events and post-market modification issues:

- If, in the iPhone example, Apple is considered a regulated entity and the iPhone is an accessory, is Apple responsible for reporting any adverse events associated with a loss in service or a dead battery?

- A loss of service may implicate AT&T, which provides wireless communication for all iPhone users. Would AT&T become a regulated entity through application of the accessory rule for providing the underlying communication technology and network infrastructure that enables the transmission of the medical device data?
- Would Apple have to report to the FDA any changes that it makes to the iPhone's operating system?

Taking this example further, consider the accessory rule's potential elevation of an mHealth component to the device classification of the parent device.

- In the Apple example, is an iPhone that is part of an mHealth system with an implantable pacemaker or defibrillator regulated, under the accessory rule, as a Class III medical device?
- What happens if the same iPhone is used as part of an mHealth system with a glucometer that is a Class II medical device?
- Does a particular iPhone model have multiple classifications based on the highest classification of the device to which the smartphone is connected? Or, does the iPhone have one classification based on the highest classification of a device to which the smartphone *could* be connected?
- Does the functionality of the smartphone app that resides on the iPhone affect the application of the accessory rule?

## **Conclusion**

The power of mHealth rests on its potential for widespread access and usability. To ensure this potential is harnessed, we must engage in a robust dialogue to determine how best to apply and interpret FDA regulations to the mHealth space. The lack of clarity surrounding the "accessory rule" poses a substantial obstacle to the growth of mHealth technology. The questions presented in this chapter are not all-encompassing, but are intended to demonstrate the complexity of the problem and the variety of the hardware components involved in any mHealth system.

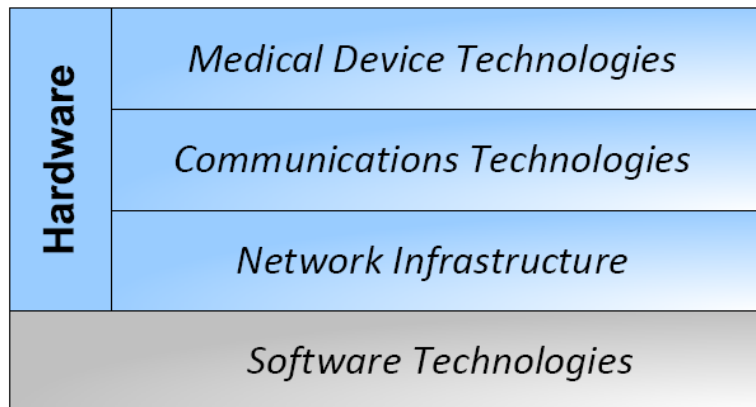
The next chapter draws our attention to the final of the four key elements of an mHealth system. Although touched on briefly in this chapter, we give software technologies particular focus because of the unique technological and regulatory features that distinguish software from hardware.

## Chapter 4

# FDA Regulation of Software Functionality in the mHealth World

In Chapter 2, we addressed various issues concerning intended uses and how a product’s uses influence whether the product is a device. In Chapter 3, we discussed the issue of connections between hardware products in mHealth, considering whether something is an “accessory” to another medical device, a stand-alone device that simply happens to talk to other devices, or not a device at all. Throughout this whitepaper, we have referred to a conceptual framework built around the four key elements into which mHealth technologies can fall.

**Figure 4.1:** The Four Key Elements of an mHealth System



In this chapter, we again review that conceptual framework. Specifically, this chapter addresses the fourth category—Software Technology—explaining what software is for the purposes of mHealth, how the FDA historically has regulated software technology, and the implications that current regulation has for the future of mHealth.

## Background: mHealth Software Applications

### Definition of Software Technologies

We begin by providing a definition of software, focusing first on what software is *not*. Remember that Chapter 3 defined hardware to include only products that could be *physically* connected, such as a sensor to a device or a device to a mobile phone. Any functionality that happens without being attributable, traceable, or linkable directly to something physical was beyond the scope of the definition of hardware and thus our discussion of the “accessory rule”.

This chapter discusses what remains. *For the purpose of this whitepaper, software functionality is defined as persistent information that includes both processing instructions and data, but that is not*

*specifically traceable or directly involved in the operation of any particular physical product itself, and is itself non-physical in nature.* In other words, if you tried to find out what “physical device” the software ran on, you would not necessarily be able to do it. Not surprisingly, software is of particular importance to mHealth because much of the storage and analysis of data being directly collected by sensors, wireless medical devices, and other physical products—most of which have their own internal software—very likely may be conducted remotely across interconnected networks through the Internet.

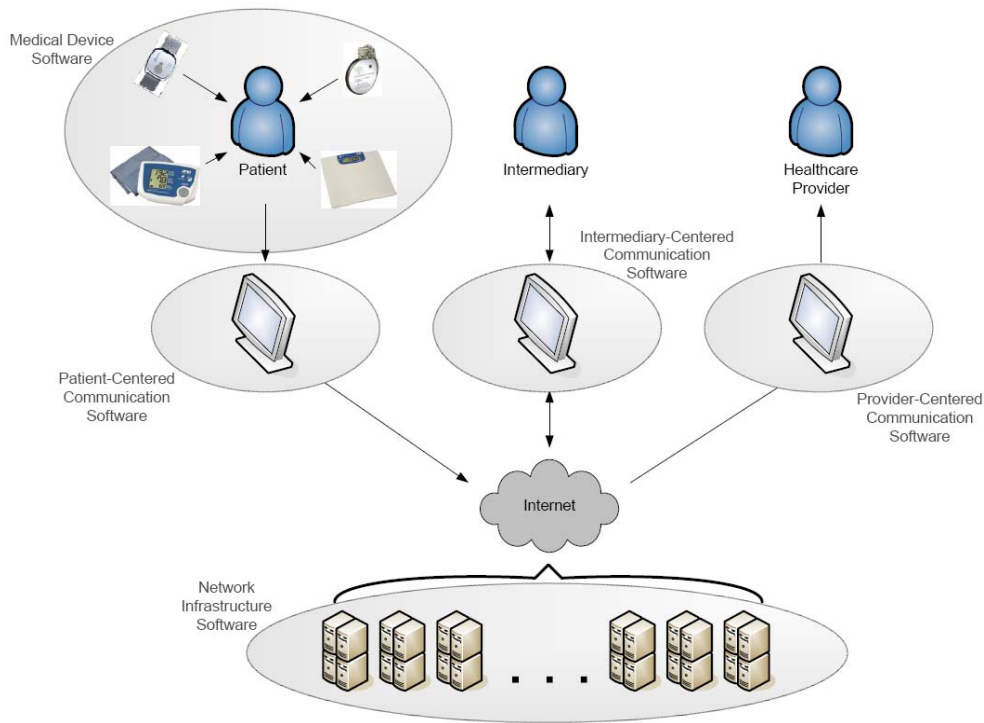
## **Hardware Components and Inherent Risk**

For purposes of analyzing the appropriate level of FDA regulatory requirements, mHealth software must be understood from two different and distinct perspectives. The first is a basic understanding of the types of software involved in the components that comprise an mHealth system. The second is a more conceptual understanding of the continuum of risk associated with the use of software with mHealth technology.

### *The Component View*

Software in the mHealth world can come in all shapes and sizes and can perform a variety of functions. Although software is purely non-physical, association with a tangible piece of hardware is required at some point throughout the web of interconnected hardware technology comprising the mHealth system. Figure 4.2 shows a simplified diagram of an mHealth system that illustrates the various elements that involve software applications, which can exist in whole or in part on any number of hardware components at any one time and can change locations at any moment.

Figure 4.2: Simplified Diagram of a Generic mHealth System



As Figure 4.2 illustrates, software can be found in any of the following mHealth components:

- Medical devices;
- Patient-centered communications technologies;
- Provider-centered communications technologies;
- Intermediary-centered communications technologies; and
- Network infrastructure technologies.

Because understanding the role of software in each of these mHealth components is helpful to understanding the FDA’s regulatory requirements for software, we describe each of them in turn.

#### Medical Device Software

Software in a medical device can come in two forms: the first is called *firmware*, while the second uses the generic *software* term. Firmware is programming code that is embedded in a device and that allows the device to function properly.<sup>46</sup> An ICD, for example, contains thousands of lines of firmware code

---

<sup>46</sup> Firmware can be found in any electronic device that contains an embedded microprocessor, including a cellular phone, a wireless router, or implantable pacemaker. The firmware code is the fundamental information that allows the machine to function and is as elemental as a resistor, capacitor, or microchip. Firmware is not within the meaning of *software* as used in this whitepaper and will not be discussed.

that sets parameters and dictates how the medical device will respond to electrical activity within the heart. Software, on the other hand, is programming code that resides on a machine, using the device to perform certain analytical tasks. A trending feature on an electronic blood pressure cuff is an example of software that resides on a medical device, using the device as a host to perform a distinct task. The trending software does not control the basic functions of the blood pressure cuff, but merely performs a discrete analytical function as an “add-on” based on the data that the blood pressure cuff collects.

#### Patient-Centered Communication Technologies

Software also can be found outside of the medical device and at any point along the information pathway from the patient to the healthcare provider. Patient-centered communications technologies (e.g., a personal computer, smartphone, tablet, or proprietary communications device, etc.) can utilize software to perform analytical tasks or to control the transmission of patient data. Microsoft Outlook, for example, could be an integral software component of an mHealth system—its function being to email alerts to the healthcare provider regarding the patient’s health status. A smartphone or tablet application is another example and may be used for displaying data trends, controlling the transmission of the information to the healthcare provider, or analyzing the data for specific disease conditions. Some mHealth systems may not use standard communications technologies but might design proprietary devices that use software in the same way.

#### Provider- and Intermediary-Centered Communications Technologies

Provider- and intermediary-centered communications technologies may be any of the same types of communications technologies used by the patient and can employ any of the types of software that are designed for patient use. The software also could be used for the same or different purposes as the patient-centered devices. An example of provider-centered software that is *different* from what a patient would use is an mHealth web application that allows the healthcare provider to access patient data for all of the provider’s patients using the mHealth system. This web app would be accessed from the provider’s personal computer and would display a variety of data collected by the mHealth system, including alert notifications, about all or a subset of the healthcare provider’s patients (e.g., only those patients who have had a recent problem). An individual patient (or family member) may have access to the same web app but would only be able to view their own patient data.

A third-party intermediary might have access to the same web app or a separate software program that allows them to view the patient data and/or create trend reports or alert notifications to be sent to the healthcare provider. In some mHealth systems, these intermediary activities could be performed automatically by software that resides on network infrastructure components, such as a computer server in an internal, secure network system or an ISP server located outside of a proprietary network. Alternatively, some mHealth systems utilize an intermediary for aggregation purposes only, allowing limited access to the patient data. In these aggregation systems, the intermediary merely compiles the data into a usable form and transmits the compiled data to the healthcare provider for review. This aggregation function may be necessary for mHealth systems that incorporate multiple stand-alone medical devices that were not originally intended to function as part of an mHealth system.

#### Network Infrastructure Technologies

The network infrastructure of an mHealth system, as discussed in Chapter 3, can include any number of servers, mainframe computers, data storage devices, wireless routers, and telephone service switches, among other things. These are distinct from the patient-, provider-, and intermediary-centered communications technologies in that the network infrastructure technologies function independently of

the other technologies and require no involvement from the patient, clinician, or intermediary. Software that resides on these components may or may not be specific to the mHealth system. For example, an mHealth system that involves an intermediary for review of patient data may include a private network of servers that stores patient data in a database and that retrieves patient data for billing and customer service purposes. The database may be an integral part of the mHealth system, while the software that retrieves data for billing and customer service purposes is not.

The software, however, need not “reside” on a network infrastructure component in the way that software is traditionally downloaded onto a computer. Cloud computing, which is becoming more common in the consumer marketplace as well as the mHealth sphere, distributes software algorithms over a number of different networked hardware components. The fluidity of this type of software system is technically powerful, promoting advanced algorithmic capabilities, but makes identifying where the software “resides” increasingly difficult. Similarly, aspects of software that once were bundled in a specific software program are now being “outsourced” across the Internet to various developers who provide “software services”. These software services perform standard functions, such as a search or payment function, across the network infrastructure and separate from any specific mHealth component.

#### *Inherent Product Risk and Intended Use*

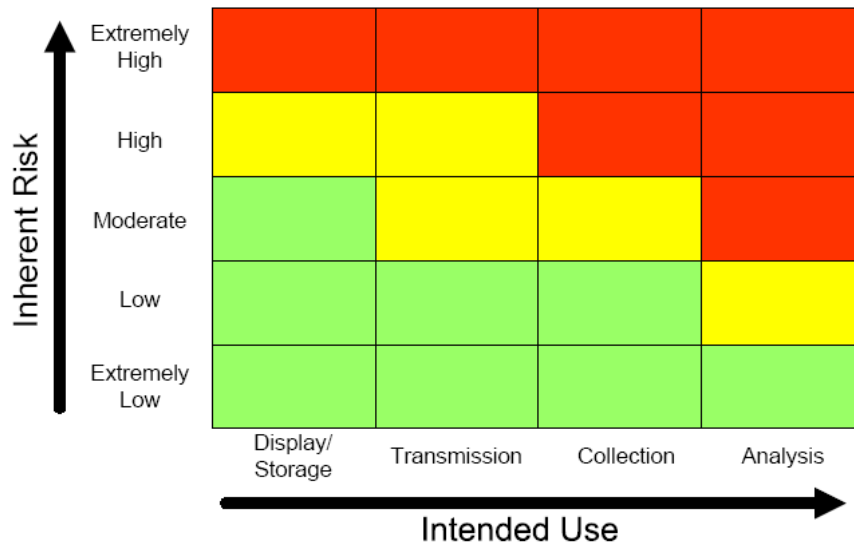
In addition to a component-centric view, software in an mHealth system should be discussed as a function of its inherent risk and intended use because these two factors influence how the product will be regulated. Generally speaking, the intended uses of mHealth software can be broken into four categories:

- 1) Display and storage;
- 2) Transmission;
- 3) Collection; and
- 4) Analysis or conversion.

Inherent risk can be broken into five categories (ranging from extremely low to extremely high) based on the severity of an adverse event occurring as a result of the use of the software. Together, these two factors are indicative of the degree of regulatory oversight that may be applicable to a given software component in an mHealth system.

Figure 4.3 shows the relationship between the intended use of a particular software component in an mHealth system and its inherent risk and how those criteria determine the significance of controls that are needed to ensure the safety and effectiveness of the software component of the overall mHealth system (i.e., red being more significant and green being less).

**Figure 4.3:** Relationship of Intended Use, Inherent Risk, and Significance of Controls for a Software Component of an mHealth System



As explained in Chapter 2, the inherent risk of a given device or product—here a specific software application—varies based on the product’s intended use. The threshold for characterizing software as a medical device and the level of controls required also depends on the intended use and inherent risk. For example, two software applications that are intended to display medical information collected in an mHealth system may be characterized differently depending on the data collected. A scale that displays an individual’s weight has an extremely low inherent risk if the individual is merely using the data for personal wellness purposes, yet the same display of the same data may have a moderate or high inherent risk if the patient is required to notify a healthcare provider when their weight reaches a certain point.

The same can be said for software that is intended to transmit, collect, or analyze patient data. The inherent risk involved with software that transmits patient data, for instance, may be dependent on the data itself, the means of transmission, and the purpose of the transmission. Consider the following examples:

- **Data itself impacting inherent risk:** Transmission of an individual’s weight may be low risk, while transmission of an alert that the patient’s weight change indicates heart failure decompensation may have a high inherent risk.
- **Means of transmission impacting inherent risk:** Data transmission from an unsecured Internet gateway directly to a healthcare provider via email may involve more inherent risk than transmission of the same data from server-to-server within a secure, private network.
- **Purpose of data transmission impacting inherent risk:** Analysis (or collection) of a patient’s weight for determining their body mass index may have a low inherent risk, while analyzing (or collecting) the same data for the purpose of predicting heart failure decompensation or the development of pulmonary edema may involve moderate or high inherent risks.

This discussion demonstrates the continuum of risk that exists for software components in an mHealth system and highlights the difficulty of regulating software in this new realm. The complexity of software architecture and functionality in an mHealth system may generate distinct risk levels for a given intended use. Furthermore, multiple software components in a given mHealth system may warrant different degrees of regulatory oversight.

## Legal Framework: Regulation of Software as a Medical Device

Although the Food, Drug and Cosmetic Act does not specifically include the term *software* in the definition of a medical device, as with any other product, the FDA regulates software as a medical device if it meets the legal definition. As explained in Chapter 2, a product meets the statutory definition of a medical device, and thus becomes subject to FDA regulatory oversight, if it is “an instrument, apparatus, implement, . . . including any component, part, or accessory, which is . . . [either] *intended for use* in the diagnosis . . . or . . . cure of disease, . . . [or] *intended to affect* the structure or any function of the body of man . . . .”<sup>47</sup>

However, as discussed in more detail below, even software that meets that legal definition might not be actively regulated. Figure 4.4 summarizes the current regulatory framework for software as a medical device.

Figure 4.4: Overview of the Regulatory Structure for Software

	Unregulated Software	Regulated Software	
Product Description	Software that does NOT meet the legal definition of a medical device.	Software that meets the legal definition of a medical device but is currently not actively regulated.	Software that meets the legal definition of a medical device and FDA is actively regulating.
Applicable Regs	None	Enforcement Discretion/ Class I Exempt	Class II/III

Let’s explore the current boundaries of FDA regulation within each of these categories.

### Unregulated Software

Software that does not meet the legal definition of a medical device is not subject to FDA authority. Again, in order not to meet the legal definition, the software must not have as an intended use the diagnosis or treatment of disease.

<sup>47</sup> Food, Drug, and Cosmetic Act § 201(h) (emphasis added).

To date, the FDA has taken the position that unregulated software includes software that automates “manual office functions . . . for the ease of the user,” such as “the report-writing functions of a computer system that allow for the manual (typewriter like) input of data by practitioners” and “software that merely performs library functions, such as storing, indexing, and retrieving information not specific to an individual patient . . . .”<sup>48</sup> The FDA has also indicated that “software that allows a doctor to enter or store a patient’s health history in a computer file” is not regulated as a medical device.<sup>49</sup>

## Regulated Software Not Subject to Premarket Clearance Requirements

### *The 1989 Draft Policy*

Since the late 1980s, the FDA has publicly declared that there exists a category of software that technically qualifies as a medical device but for which the FDA has no intention of requiring the submission of a premarket notification or approval application.<sup>50</sup>

In 1989, the FDA established exemptions from regulatory oversight for two categories of software:

- 1) General purpose articles as defined in a regulation; and
- 2) Software that involves competent human intervention.<sup>51</sup>

The first category, *general purpose articles*, covers “laboratory equipment whose uses are generally known by persons trained in their use and which are not labeled or promoted for medical uses.”<sup>52</sup> Additionally, via the classification process, the FDA has adopted specific general purpose or low risk exemptions that cover software. These exemptions include laboratory information management systems used as calculators or data processing modules for clinical use.<sup>53</sup> Although the second category of software involving *competent human intervention* is often cited, the FDA never actually codified the exemption.

About seven years after the FDA published the 1989 draft policy, it appeared the FDA was moving toward formalizing its computer product policy. In addition to publicly announcing that intention, the FDA hosted a large meeting in Washington and invited many stakeholders to discuss what the policy should be. In preparing for that meeting, the FDA drafted a summary of what it considered to be its then-existing policy on computer products. Those workshop materials explained that much of the software the Agency was seeing constituted accessories to medical devices, and the competent human intervention concept was only intended to apply to truly stand-alone software. The Agency also argued that the concept of what constitutes competent human intervention had become increasingly complex and difficult to administer. The FDA observed:

---

<sup>48</sup> Devices: General Hospital and Personal Use Devices; Reclassification of Medical Device Data System, 73 Fed. Reg. 7498, 7500 (Feb. 8, 2008).

<sup>49</sup> *Id.*

<sup>50</sup> EHR systems, for example, have historically been considered medical devices but the FDA has used its enforcement discretion to refrain from active regulation.

<sup>51</sup> FDA Policy for the Regulation of Computer Products, 11/13/89 Draft.

<sup>52</sup> 21 C.F.R. § 862.2100.

<sup>53</sup> *Id.* § 807.65.

In general, to permit competent human intervention, the software decision process must be completely clear to the user, with a reasonable opportunity for challenging the results. There must also be adequate time available for reflection on the results.

But again, the FDA never adopted a new regulation or policy.

### *Medical Device Data Systems*

Most recently, in early 2008, “[the] FDA realized that the [1989] Draft Software Policy was not adequate to address all of the issues related to the regulation of computer based and software based medical devices.”<sup>54</sup> The Agency proposed a new category of software—called *Medical Device Data Systems* (MDDS)—that would fit within this general category of regulated software exempt from premarket clearance as a Class I device. The FDA defined MDDS to include the following:

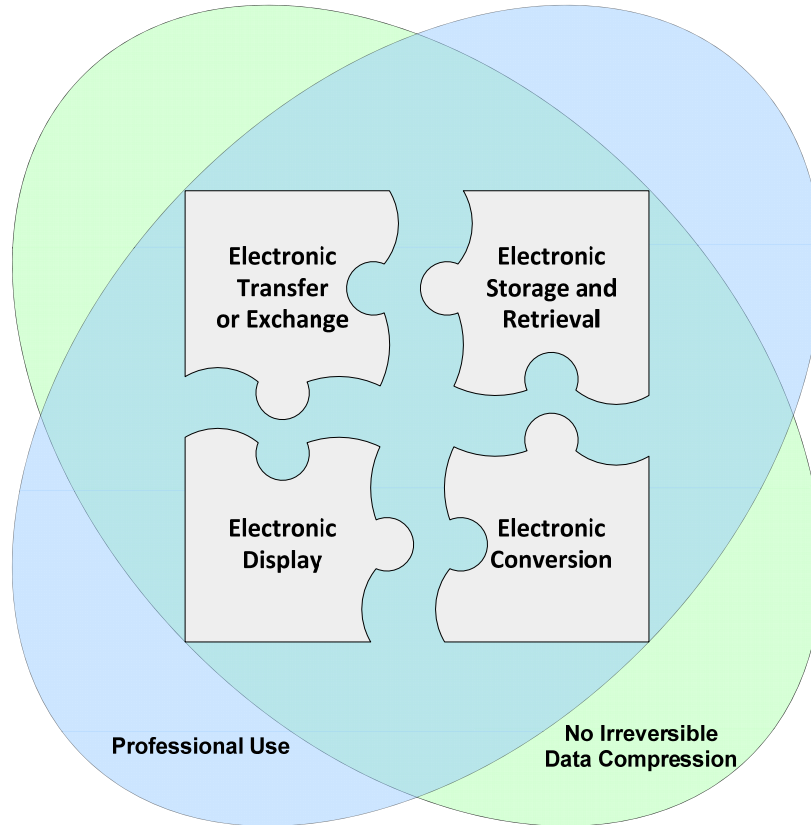
- The **electronic transfer or exchange of medical device data** from a medical device, without altering the function or parameters of any connected devices. For example, this would include software that interrogates a ventilator every fifteen minutes and transfers information about patient CO<sub>2</sub> levels to a central patient data repository.
- The **electronic storage and retrieval** of medical device data, without altering the function or parameters of connected devices. For example, this would include software that stores historical blood pressure information for later review by a healthcare provider.
- The **electronic display** of medical device data, without altering the function or parameters of connected devices. For example, this would include software that displays the previously stored ECG for a particular patient.
- The **electronic conversion** of medical device data from one format to another format in accordance with a preset specification. For example, this would include software that converts digital data generated by a pulse oximeter into a digital format that can be printed.

MDDS is proposed only to be available as an exemption from premarket clearance so long as the data set is **intended for professional use and does not produce irreversible data compression**.

---

<sup>54</sup> Devices: General Hospital and Personal Use Devices; Reclassification of Medical Device Data System, 73 Fed. Reg. at 7499.

**Figure 4.5:** Proposed Medical Device Data Systems Regulation



To further understand how the proposed MDDS regulation applies to mHealth technologies, let’s look at the details more closely. The proposed rule explains that “[e]xamples of [MDDS] that would be used in the home are systems that periodically collect data from glucose meters or blood pressure devices for later review by a healthcare provider.”<sup>55</sup> The rule limits MDDS to software systems that “are not intended or designed to provide any real time, active, or online patient monitoring functions.”<sup>56</sup> While MDDS can “deliver and store alarm data,” such systems “do not have the capability to display, create, or detect alarm conditions, or to actually sound an alarm. In particular, a[n] MDDS can record the fact that an alarm sounded, but cannot by itself sound an alarm in response to patient information” or “create alarms that are not already present from the connected medical devices.”<sup>57</sup> Finally, MDDS are not designed to “provide any diagnostic or clinical decision making functions” but “can transmit, exchange, store, or retrieve data in its original format” or can convert data “from one format to another,” such as

---

<sup>55</sup> *Id.* at 7500. The rule defines *medical device data* as “numerical or other information available from a medical device in a form suitable for processing by computer” and explains that these data “can represent many types of information (e.g., clinical values, alarm conditions, error messages).” *Id.*

<sup>56</sup> *Id.*

<sup>57</sup> *Id.*

arranging or organizing data based on “preset specifications.”<sup>58</sup> The proposed regulation does not define or clarify the preset specifications.

As of this writing, the Agency has not issued the MDDS proposed rule in final form. Recent pronouncements by the Director of the FDA’s Center for Devices and Radiological Health suggest that a final rule may be published by the beginning of 2011. For the time being, however, it seems to be the best guidance available for deciding whether a premarket clearance is required for software in an mHealth system.

## **Software Requiring FDA Premarket Clearance or Approval**

The third and final category—software that meets the definition of a medical device and that is actively regulated—requires premarket clearance or approval from the FDA. Although the classification of software in this category may seem to be the most obvious of the three general categories, the process of determining which regulation or policy applies is complicated by the fact that the word *software* is contained in 431 of the nearly 1700 classification regulations.

The FDA describes *software devices* that require premarket clearance or approval as products that contain one or more software components or are composed solely of software, including:

- Firmware and other means for software-based control of medical devices;
- Stand-alone software applications;
- Software intended for installation in general-purpose computers;
- Dedicated hardware/software medical devices; and
- Accessories to medical devices when those accessories contain or are composed of software.<sup>59</sup>

In addition, the proposed MDDS regulation indicates that “MDDS devices indicated for lay use or that perform irreversible data compression [should] not be exempt from premarket notification requirements.”<sup>60</sup>

As with other devices requiring premarket clearance or approval, the software that falls into this category must comply with general controls, such as Good Manufacturing Practices, medical device reporting, and correction and removal requirements. The FDA also may apply special controls for devices, including software, that require premarket clearance. The special controls are typically stated in FDA guidance documents and include, for example:

- Guidance for Industry – Wireless Medical Telemetry Risks and Recommendations;
- Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices;

---

<sup>58</sup> *Id.*

<sup>59</sup> Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 2005).

<sup>60</sup> Devices: General Hospital and Personal Use Devices; Reclassification of Medical Device Data System, 73 Fed. Reg. at 7500.

- General Principles of Software Validation; Final Guidance for Industry and FDA Staff;
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices;
- Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software; and
- Device-specific guidance (e.g. glucose monitors).

Within this category, the specific classification of the software also dictates the level of validation required. If the software is an accessory, the parent device determines the level of validation required. If not an accessory, the validation required depends on the “level of concern” that the FDA associates with the software, as described in Figure 4.6.<sup>61</sup>

**Figure 4.6:** Level of Concern Associated with Regulated Software that Is Not an Accessory to a Medical Device

<b>Level of Concern</b>	<b>Major:</b> The software directly affects the patient or anyone else such that a failure could result in death or serious injury.
	<b>Moderate:</b> The injuries would be non-serious.
	<b>Minor:</b> Failures would not be expected to result in any injury.

The FDA evaluates the inherent risk and level of concern associated with the software to determine:

- The depth and degree of hazard analysis and mitigation that is expected;
- The depth and degree of documentation;
- What needs to be submitted as opposed to simply documented;
- The rigor applied to the verification and validation of the software; and
- The degree to which the device manufacturer’s software development process is scrutinized.<sup>62</sup>

Further, the FDA has taken enforcement action against software developers who have failed to obtain premarket clearance or approval for their products. For instance, the Agency has issued a number of

---

<sup>61</sup> Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 2005); Guidance for Industry, FDA Reviewers and Compliance on Off-The-Shelf Software Use in Medical Devices (Sept. 1999).

<sup>62</sup> Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices (May 2005).

Warning Letters relating to the unapproved marketing of software devices, representative examples of which include:

- *Digisonics, Inc. (1996)*: The FDA cited the unauthorized manufacture and distribution of software used in conjunction with cardiac diagnostic and fetal growth development systems, specifically noting a failure to establish and implement adequate quality assurance procedures to address changes to the software.<sup>63</sup>
- *Individual Monitoring Systems, Inc. (1999)*: The FDA cited the ActiTrac Activity Monitor, Display and Analysis Software and its Sleep Scoring Program because the “claims represent[ed] or suggest[ed] that the [software] devices are used to monitor or provide physiological data to evaluate a patient's medical condition (i.e., insomnia) for diagnosis and treatment of a sleep disorder.”<sup>64</sup>
- *AvidCare Corp. (2001)*: The FDA cited a failure to obtain premarket clearance or approval for the company's Home Health Monitoring Systems and associated software, which were deemed to be medical devices because they “use[d] spirometry for in-home monitoring of asthma.”<sup>65</sup>
- *Lexicor Medical Technology Inc. (2003)*: The FDA cited the company's “DataLex’ web portal”, which had been promoted as being able to diagnose Attention Deficit Hyperactive Disorder in humans.<sup>66</sup>
- *Biolmagene, Inc. (2005)*: The FDA cited the company's “hardware-independent, Web-enabled software [that] allow[ed] pathologists to view and analyze immunohistochemically-stained . . . slides from any computer via the Internet.”<sup>67</sup> The Agency found the unapproved marketing of the software as “an intelligent image analysis software system designed to fulfill the needs of objective analysis of oncopathology images” and “caters to the smarter diagnostic practices needed by researches, oncopathologists, and physicians . . . .”<sup>68</sup>
- *Seryx, Inc. (2007)*: The FDA determined the company's Signature Genetics software to be a device because the software was “used to analyze data and generate a patient-specific report via . . . interpretation of a patient's genotype for several drug metabolizing enzymes.”<sup>69</sup>

These enforcement actions are examples of the broad approach the FDA takes to the regulation of software as a medical device. The Agency has regulated Internet sites, in-home monitoring systems, and imaging software as medical devices, while at the same time exempting certain categories of systems

---

<sup>63</sup> FDA Warning Letter to Diana McSherry, Chairman and CEO, Digisonics, Inc., Nov. 14, 1996, *available at* <http://www.fda.gov/downloads/ICECI/EnforcementActions/WarningLetters/1996/UCM065074.pdf>.

<sup>64</sup> FDA Warning Letter to David T. Krausman, Vice President and CEO, Individual Monitoring Systems, Inc., July 28, 1999, *available at* <http://www.fda.gov/downloads/ICECI/EnforcementActions/WarningLetters/1999/UCM067527.pdf>.

<sup>65</sup> FDA Warning Letter to Boaz Avitall, Chairman and CTO, AvidCare Corporation, Apr. 17, 2001, *available at* <http://www.fda.gov/downloads/ICECI/EnforcementActions/WarningLetters/2001/UCM069569.pdf>.

<sup>66</sup> FDA Warning Letter to Stephen N. Xenakis, President and CEO, Lexicor Medical Technology Inc., Jan. 16, 2003, *available at* <http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2003/ucm147274.htm>.

<sup>67</sup> FDA Warning Letter to Mohan Uttarwar, President, Biolmagene, Inc., *supra* note 22.

<sup>68</sup> *Id.*

<sup>69</sup> FDA Warning Letter to Patrick Rambaud, President and CEO, Seryx, Inc., *supra* note 21.

such as an MDDS or general purpose article. The difficulty that mHealth technology companies face is determining when premarket clearance or approval is required. Below we discuss some of the challenges that these companies face in making this determination due to the complexities of the software technologies that form the basis of mHealth systems.

## Challenges: Applying the Appropriate Regulatory Requirements

The distinctions just discussed represent the current state of a regulatory environment that has already struggled to keep pace with the rapid evolution of how software is used as, and in connection with, medical devices. As mHealth technologies continue to develop, we expect the gap between the current regulatory framework and the state of the art to expand even more. Some of the questions that must be addressed to bridge this gap are presented below.

### What Software Is Regulated as a Medical Device?

#### *Software that Automates a Function for Ease-of-Use*

As noted above, the FDA has said that software that merely automates a function for ease-of-use is not regulated as a medical device. Consider the following:

- How would the FDA classify software that sends notifications to a patient to take a pill or to remind them to visit their healthcare provider?
  - Is such software not regulated as a medical device because it is simply automating the function of a healthcare provider (e.g., a physician, nurse, or pharmacist) who would normally contact the patient to remind them?
  - If it is regulated as a medical device, would the software be classified under the MDDS proposed rule as a Class I device exempt from premarket notification requirements?
- Does the physical location of the software dictate whether and to what extent the product is regulated as a medical device?
  - If the software system is intended to function in the patient's home rather than the healthcare provider's office, is the software subject to regulation as a medical device even if it merely automates a function for ease-of-use? What if the software system is located on an intermediary computer or server?

#### *Software that Performs Library Functions*

Software that merely performs library functions, such as storing, indexing, and retrieving information not specific to an individual patient, also historically has not been regulated as a medical device. Consider the following:

- Is a web app that retrieves data from a manufacturer's database/server in order to display alerts and patient information for all of a healthcare provider's ICD patients regulated as a medical device if the storing, indexing, and retrieving process is not specific to an individual patient?

- If the web app is regulated as a medical device, would the device classification depend on whether the web app used standard protocols and standardized web services as opposed to proprietary ones?
- Is a software app stored on a proprietary communication device located in the patient's home regulated as a medical device if it asks the patient questions and transmits the patient's answers to a healthcare provider?
  - If such software is a medical device, does the device classification depend on the types of questions being asked and the purpose of those questions, even though the processes for posing the questions and transmitting the answers are identical?

### *Provider-Derived Software*

An area of increasing uncertainty is the regulation of provider-derived software that performs mHealth functions. The FDA has historically exercised its enforcement discretion to refrain from regulating EHR and EMR systems. Many mHealth systems, however, connect to EMR and EHR systems established in a given healthcare facility, generating the following questions:

- Would the connection to an mHealth system subject a provider-derived software system to regulation as a medical device if the systems are intended to connect? If so, what classification would apply?
  - What if the systems use standard protocols to connect to each other?
- If the entire mHealth system, including the software components, is developed within a healthcare facility, is the system subject to regulation as a medical device? If so, is the classification the same as a system that is derived outside of the healthcare facility?

## **What Software Is a Device, But Is Exempt from General Controls and Premarket Notification?**

### *Software as a General Purpose Article*

Software that qualifies as a general purpose article that is not labeled or promoted for a medical use and has a use generally known by persons trained in its use is exempt under 21 C.F.R. § 807.65 from device registration requirements.

- How far does the general purpose article exemption extend?
  - For example, if an mHealth system incorporates a computer or smartphone to allow a healthcare provider access to patient data via a web app server, is the computer a general purpose article?
  - If so, is the Internet server that allows the computer to access the web application server exempt from device registration requirements as a general purpose article?
  - If so, is the web app exempt?

- If the web app is executed in a cloud computing network, does the general purpose article exemption apply to the software and all components that might execute a piece of that software?

### *Software Involving Competent Human Intervention*

Software that involves competent human intervention also has been considered exempt from premarket notification requirements under the 1989 draft policy.

- Does this exemption still exist? If so, what constitutes “competent human intervention”?
- Would a third-party intermediary who is a trained clinician (e.g., physician, nurse, or other healthcare provider) qualify under this exemption?
- Does software that allows that intermediary to view patient data and make decisions whether to send alert notifications to the healthcare provider qualify under this exemption?
- Does the competent human have to be a trained clinician (e.g., physician, nurse, or other healthcare provider)? If the software simply requires that the patient click a button to send data to their healthcare provider, will the software qualify for this exemption?

### *Software Involving MDDS*

MDDS software that is intended for professional use and that does not produce irreversible data compression has been proposed to be Class I exempt from premarket clearance requirements. Consider the following:

- What classification applies to software that is intended for use by a lay person?
  - Does the “professional use” requirement mean that *any* licensed professional (e.g., nurse, physician assistant, or other healthcare provider) can access the data or is the scope limited to that of a physician? For example, if an mHealth system uses software that is stored on an intermediary’s server system for review by trained clinical staff prior to transmission to the patient’s healthcare provider, is the software regulated as a medical device under the MDDS proposed rule?
- What classification applies to software that performs some irreversible data compression?
  - Does the “no irreversible data compression” requirement apply if software in an mHealth system displays data as a trend or analyzes data in some other fashion that does not change the original data?
- If an mHealth system incorporates software that periodically collects and aggregates data from multiple devices and transmits that data for review by the patient’s healthcare provider, does that software fall within the MDDS Class I exemption?
  - Does the aggregation function constitute an electronic conversion within the meaning of MDDS?
  - If the data from the multiple devices are displayed together in one screen or report, does this constitute an electronic display within the meaning of MDDS?

- How is a software device classified if it is designed or intended to provide real-time or active remote patient monitoring and, therefore, does not fall within the proposed Class I category for MDDS?
  - What is considered “real-time” or “active monitoring” in this context? How frequently can an mHealth system transmit data and still be within the MDDS proposed rule?
- What classification would software receive if the mHealth system notifies a healthcare provider of an alert condition?
  - What if the software simply transmits the existence of an alert on the medical device?
  - What if a third-party intermediary reviews medical device data and uses software to notify a healthcare provider of an alert condition?
- What classification would software receive if the mHealth system notifies the patient of an alert condition? What if the software notifies a family member of the patient?
  - Does the answer depend on the content or the purpose of the alert? For instance, is the classification different if the alert notifies the patient of the need to take a pill or that the patient has a scheduled physician appointment as compared to notifying the patient that they have *missed* a required pill or appointment?
  - Does the classification change if the software notifies a third-party intermediary who subsequently contacts (via phone or other means of communication) the patient or physician of the alert condition?
- What classification would apply to software in an mHealth system that transmits the diagnostic or clinical decisions made by a trained intermediary?

## **What Software Is Regulated as a Device by Virtue of the Accessory Rule?**

The ambiguity of the accessory rule has significant implications on the regulation of software. The questions addressed previously in Chapter 3 apply here and will, therefore, not be repeated. Suffice it to say that questions remain regarding smartphone manufacturers and Internet Service Providers, among others, because it is unclear how the accessory rule applies to software applications. Specifically, regulation of software that resides on a smartphone or that uses a “cloud” of networked computers and servers may implicate the manufacturers of the hardware components. If and when the accessory rule breaks down in the mHealth context, the current rules for regulating software also fail because they cannot cover the complexity of the software architectures and the variety of mHealth systems that are under development and that continue to evolve. Where software once was considered a medical device under the accessory rule, the challenges presented draw into question the appropriateness of such a classification.

Consider the following questions regarding the application of the current accessory to software:

- For what purposes can a software application access medical device data without being considered an accessory?

- Is a software app that enables a device manufacturer to review patient data for billing or customer service purposes an accessory by virtue of the connection to the manufacturer's device?
- Is software that forms the basic operating systems of the various hardware components (e.g., computers, smartphones, and servers) regulated as an accessory if the hardware component is regulated as an accessory?
- Is software that is otherwise unregulated as a medical device subject to the accessory rule?
- Is software that falls within the MDDS proposed classification subject to the accessory rule?

## What Software Is Regulated as a Device that Requires Premarket Clearance?

Software that is considered a medical device but is not an accessory is regulated under the inherent risk and level of concern analysis. The following questions demonstrate the uncertainty that surrounds this analysis:

- Does the analysis change based on the intended location of the software within the mHealth system?
  - For instance, is a software app that runs on a smartphone and provides emergency notifications directly to the healthcare provider of a greater or lesser risk/concern than the same software app that resides on the healthcare provider's office computer, where notification might not be as immediate?
  - Does the answer change if the software does not "reside" anywhere?
- Similarly, does the software communication functionality affect the regulatory oversight?
  - For instance, is software that uses an email notification service regulated differently than software that sends text messages?
  - Is the content of the email or text message relevant given length limitations?
  - If the notification simply informs the healthcare provider to contact the patient or informs the patient to contact the healthcare provider, does the software involve more or less risk and concern than if the notification provided specific patient data?
- Does the software classification depend on the classification of the hardware component on which the software executes?
  - For instance, if a computer is considered an accessory to a Class II medical device, does downloading software to that computer subject the software to Class II regulation? Does the answer depend on the intended use of the software?
  - What classification would apply if the software does not "reside" on any specific device?

## Conclusion

As demonstrated in the discussion in the chapter, the changing landscape of software development and the intangibility of software itself makes regulation in the mHealth sphere more and more difficult as the technologies advance. Software is an integral component of any mHealth system and obtaining clarity and predictability around how the FDA will regulate in this space is essential to continued growth and innovation. The public health advances that come with the growth of mHealth technologies justify the discussion and effort necessary to establish clear and predictable regulatory guidelines for associated software technologies.

## Chapter 5

### Conclusion: Innovation and the Impact of Regulation

The advancement of public health is a mission shared by the FDA and developers of mHealth technologies. Innovation within the mHealth industry has grown rapidly in recent years primarily due to the development of the Internet as well as the availability of high-speed mobile and wireless communication technologies and the hardware and software equipment that enable individual consumers to “stay connected” from virtually anywhere and everywhere.<sup>70</sup> In the same way that social media tools (e.g., Facebook and Twitter) have broken the traditional barriers of communication in our society, mHealth technologies (through mobile and wireless communications systems) have empowered physicians and their patients with the freedom of delivering and receiving healthcare outside of the confines of a traditional healthcare facility. With the growing cost pressures in healthcare, the increasing familiarity with mobile devices, and the ever-expanding population of patients with chronic disease conditions, mHealth technologies have become, and will continue to be, a vital component of the healthcare system in the United States.

The FDA plays an essential part in the growth of the mHealth industry and the delivery of mHealth technologies. The Agency acts as a check on industry to ensure that technological development does not come at the expense of the safety and effectiveness of products that reach the market. To date, the FDA has relied primarily on the existing framework for medical devices to regulate mHealth technologies. Unfortunately, the established framework fails to address adequately many of the aspects of mHealth systems that make the technology powerful.

In this whitepaper, we have attempted to identify the areas where improved clarity and guidance from the FDA is necessary to ensure the continued growth of the mHealth industry and the delivery of mHealth technologies to patients and healthcare providers. First, we established a definition of *mHealth* and provided descriptions of the four key elements that form the fundamental architecture of an mHealth system. Next, we discussed in detail the three areas of primary concern: 1) intended use; 2) connected hardware; and 3) software functionality.

To briefly review, the question of intended use in mHealth poses a significant concern for the future of the industry because a product’s intended use forms the basis upon which the FDA has authority to regulate. The Agency’s authority is limited, in relevant part, to products intended for use to diagnose or treat a medical condition. Many mHealth products currently are designed to address general health and wellness problems, and the dividing line between wellness and medical diagnosis or treatment is unclear. This whitepaper presented a number of questions that highlight the need for clarity.

Next, regulation of hardware components within an mHealth system is the second key area in which the current regulatory framework fails to provide clear guidance. An mHealth system is composed of a myriad of hardware components that work in concert to perform various data collection, storage,

---

<sup>70</sup> The summit of Mt. Everest—the highest point on Earth—recently became one of the most wirelessly accessible locations on the planet.

display, analysis, and transmission functions. These components interact through wired and wireless connections that rely on both standard and proprietary communications protocols. Many of these components are designed and developed beyond the reach of the mHealth system manufacturer and may be controlled by national standardization bodies or large corporations. As such, regulation of these components of an mHealth system—and how practically to comply with any FDA requirements—poses significant challenges.

Third and finally, the regulatory framework that applies to software within an mHealth system is uncertain. Historically, software with specifically defined features has been regulated as a medical device; at the same time, the FDA has not finalized several rules that would establish basic guidelines for the regulation of software as a medical device and has not published an mHealth-specific app guidance document. As with the other areas discussed in this whitepaper, the mHealth industry thirsts for guidance from the FDA on how the Agency intends to regulate the software component of mHealth technology. The lack of clear guidelines creates significant uncertainty that will hinder the innovative spirit of the mHealth industry if the regulatory ambiguity persists.

For these reasons, the mHealth Regulatory Coalition has developed this whitepaper and hopes to begin a discussion between mHealth stakeholders and the FDA regarding the regulation of mHealth technologies. Ultimately, we hope that this discussion will result in the development of a guidance document that provides a clear and predictable regulatory pathway that fosters innovation and ensures the safety and effectiveness of mHealth technologies.

The task of developing such a guidance document parallels the Agency's recent efforts to establish guidelines for dietary supplements. Prior to the growth of the dietary supplement industry, medical science did not truly understand the relationship between diet and health. As development of new dietary supplements illuminated the relationship with improved overall health, a dialogue began on the impact on specific diseases or conditions. The discussion of specific diseases or conditions required the FDA to address the potential for a dietary supplement to become a drug under the Food, Drug and Cosmetic Act. Congress finally entered the discussion and amended the Agency's statutory authority to allow consumers to make informed decisions about the use of dietary supplements to improve their health.

Although the regulation of mHealth technology follows a similar path as dietary supplements, a statutory amendment is not required because the FDA currently has the authority to establish a clear regulatory framework upon which the mHealth industry can rely. Where these two examples are similar, however, is in the need for freedom to discuss the health benefits of wellness products, specifically where clear medical consensus exists around a particular health condition. The ability to make marketing statements based on clear medical consensus will enable the widespread use of mHealth technologies, thereby improving public health through education and use of these technologies. The FDA and the guidance documents that the Agency establishes play a vital role in this endeavor.

# Appendix

## List of Abbreviations

Act	Food, Drug and Cosmetic Act
App	Software or Web Application
BAN	Body Area Network
CCR	Continuity of Care Record
DAS	Distributed Antenna System
DSL	Digital Subscriber Line
ECG	Electrocardiogram
EHR	Electronic Health Record
EMR	Electronic Medical Record
FDA	Food and Drug Administration
ICD	Implantable Cardioverter Defibrillator
ISP	Internet Service Provider
LAN	Local Area Network
LTE	Long-term Evolution
M2M	Machine to machine
MCOT	Mobile Cardiac Outpatient Telemetry
PAN	Personal Area Network
PDA	Personal Digital Assistant
PHR	Personal Health Record
PSTN or POTS	Public Switched Telephone Network or Plain Old Telephone Service
RFID	Radiofrequency Identification
RTLS	Real-time Locating System
SMS	Short Message Service