eSource in Clinical Research: A Data Management Perspective on the Use of Mobile Health Technology

A White Paper

September 30, 2016

Society for Clinical Data Management

Table of Contents

Acknowledgments iii

1. Foreword 1

2. Abstract 1

3. Introduction 1

4. Evaluating mHealth Technologies 3

5. Managing Study Risk 12

6. People and Processes...13

7. Standards for mHealth..17

8. Regulatory Landscape..19

9. Conclusion 20

10. References...20

Appendix: Mobile Standards to Facilitate Data Collection, Exchange, and Security 25

Acknowledgments

The Society for Clinical Data Management (SCDM) would like to thank the following individuals who collaborated on the SCDM Clinical Data Innovation Committee to produce this manuscript.

Authors: Linda King (Chair), Sunil Agarwal, Sanjay Bhardwaj, Ann Delaney Fleenor. , Henry Friend II, Begoña Gonzalez, Ralph Russo, Erica Sage, Candace Friend Shelton, Matt Southwick, Roger Stuedemann, Dorian Tisdale, Susan Tunstall and Anita Walden

The SCDM Clinical Data Innovation Committee would like to offer their appreciation and special thanks to:

- The many individuals and organizations who offered their feedback and comments during the public comment period
- The FDA for their encouragement with regard to this paper and the topic of mHealth.
- The SCDM Board of Trustees for their feedback and support for the Clinical Data Innovations Committee and this publication
- Liz Wing, MA, for editorial assistance
- SCDM Clinical Data Innovation Committee including Charlene Dark, Paul Grady, Ioannis Karageorgos, Derek Perrin, Osman Qamar, Guang-liang Wang, and Demetris Zambas
- Richard A. Bloomfield, Jr., MD from Duke Health and Ryan Jeffrey Shaw, PhD RN from Duke School of Nursing

Disclaimer: Not all the views expressed in this white paper may be those of the individual companies or entities for which authors are employed or affiliated.

1. Foreword

The Society for Clinical Data Management's (SCDM's) Clinical Data Innovation Committee is a newly formed committee evolving from the eSource (electronic source data)/EDC (Electronic Data Capture) Task Force, which authored SCDM's *eSource Implementation in Clinical Research: A Data Management Perspective* white paper in June 2014.[1] The Clinical Data Innovation Committee is a think tank and future-minded group exploring a new data source for data professionals called mobile health technology, also known as mHealth. Building on the original white paper's seven principles and electronic clinical outcomes assessment (eCOA) sections, the Committee explored strategic and practical implications of mHealth technologies for data managers. Topics addressed in the present paper cover considerations for and impact to business processes, roles, standards, regulations, and the mHealth technologies themselves that may be used for clinical research.

The goal of this paper is to provide data management professionals with a framework to evaluate and implement mHealth technologies using eSource principles. In this paper, we introduce mHealth technology as it relates to the data management discipline, and we hope to stimulate discussion of mHealth to continue SCDM's dialog on eSource and clinical data innovation.

2. Abstract

Electronic source data (eSource) in the form of mHealth technologies used for study participant data collection is gaining momentum within the clinical research setting. To effectively adopt mHealth technologies as new data sources, we propose a principles-based approach to the evaluation of eSource, as outlined in the following key areas: technology, people, processes, and standards. We also outline regulatory considerations to provide general guidelines for adoption. All roles, participants, and processes in the clinical trials enterprise will be affected by changes in technology involving new standards, data flows, and data sources. Clinical data managers will see their roles expand and will be positioned to drive the process changes necessary for adopting successful mobile technologies. Mobile health will be a game changer in the conduct of clinical research—one that benefits both the trial participants and the research.

3. Introduction

This paper builds on the eSource principles-based approach from SCDM[1] to address, from a data management perspective, the implications of using mobile health (mHealth) data in clinical research. Mobile health is a timely topic: The National Institutes of Health (NIH) Consensus Group states that, "mHealth is the use of mobile and wireless devices to improve health outcomes, healthcare services and health research," and market analysis reports show there is an accelerated growth of the use of mHealth technologies, with sales expected to bypass those of desktop computers, PCs, and desktops.[2] Adapting to online and mobile technologies is no longer a novelty: one area shown to have the sharpest increase in the adaptation of mobile technology is the health and fitness space.

As described by the NIH, "the recent proliferation of wireless and mobile technologies provides the opportunity to connect information in the real-world via wearable sensors and, when coupled with fixed sensors embedded in the environment, to produce continuous streams of data on an individual's biology, psychology (attitudes, cognitions and emotions), behavior and daily environment. These data have the potential to yield new insights into the factors that lead to disease. They also have the potential to be analyzed and used in real time to prompt changes in behaviors or environmental exposures that can reduce health risks or optimize health outcomes."[3,4] Mobile health is becoming a transformative force with the potential to change when, where, and how healthcare is provided, and to ensure that important social, behavioral, and environmental data are used to understand the determinants of health and improve health outcomes.[5]

The U.S. Food and Drug Administration (FDA) also has recognized the changes taking place, stating that, "As mobile platforms become more user friendly, computationally powerful, and readily available, innovators have begun to develop mobile apps of increasing complexity to leverage the portability mobile platforms can offer. Some of these new mobile apps are specifically targeted to assisting individuals in their own health and wellness management. Other mobile apps are targeted to healthcare providers as tools to improve and facilitate the delivery of patient care."[6,7]

Throughout this document, we use the term mHealth to mean the variety of technologies that involve mobile medical or health applications, telemedicine devices, and telehealth—essentially forms of electronic devices available to the patient and operating either independently or in connection with a medical facility.

When linked via an mHealth app to a smartphone or smartwatch, health data can be made available in real time for use in clinical trials. Technology advancements have sharply increased the introduction of applications and wearable devices from major technology companies.[8] (e.g., HealthKit®, Google Fit® and ResearchKit® [9-12] For example, large technology companies are capitalizing on the powerful processors and advanced sensors that mobile phones currently have that can track movement, take measurements, and record information (e.g., HealthKit®, Google Fit®, ResearchKit®, Substitutable Medical Applications and Reusable Technologies (SMART) on HL7 Fast Healthcare Interoperability Resource FHIR® platform®).[9-12]

Due to this increased focus on the healthcare domain, it seems natural for the medical research community to use mHealth to collect evidence to support research and to take advantage of mHealth's multiple benefits. Yet while new technology can potentially enhance the experience of clinical trial participants and improve efficiencies in clinical trials (**Table 1**), it can also present some challenges (**Table 2**).

Table 1. Benefits of mHealth Technology

Participant Benefits	**Clinical Trial Benefits**
Opportunity for increased access to participant's own data	Increased real-time data access
Increased opportunity for trial participation	Increased enrollment and inclusion of diverse populations
Decrease the frequency of in-person site visits	Increased objective data via direct collection to mobile device (i.e., heart rate)
Reduced burden of data collection	Potential reduction of cost over time
Potential increased participant adherence to the protocol	Secondary use for other research purposes
Potential increase satisfaction with trial participation	Investigator time more focused on direct intervention
Patient engagement	Patient-CenteredTrials

Table 2. Challenges of mHealth Technology

Learning curve for sponsor and site staff on how to implement mHealth technologies
Regulatory policies/standards still in development
Using the right technology and vendors
Participants’ acceptance of mHealth technology for clinical trial use
Privacy and security considerations
Collection of the right data to support analysis
Attributability and potential fraud
mHealth tools validation
Possible different rates of acceptance among different age groups
Potential increase costs for development such as user support, possible increased security risk to protected health information
Need for data standards due to variations in data across tools

The following sections highlight the benefits and best practices of using mHealth and also consider the risks and challenges.

4. Evaluating mHealth Technologies

The mHealth landscape is broad and covers a variety of technologies to accommodate the different types of data collection and retrieval needs in clinical trial and healthcare settings (**Table 3**). The number of options within each technology is vast. For example, several types of health-based applications are available for use from major companies, with Android and Apple together providing more than 100,000 health apps.[10,12]

When implementing mHealth technologies in a clinical study, the selection process is complex because it entails the evaluation of the device model itself, the vendor who created the device, the applications to be used, the algorithms for collecting/processing the data, the method of data transmission, global coverage and device technology support, and the communication provider companies involved with the data transmissions. The selection of any device or service should provide confidence for the integrity of the data originating from the device/service. Understanding the data chain of custody—from collection and transmission to storage within your organization—will be key to ensuring data security, integrity, quality, and privacy.

Table 3. mHealth Technologies: Devices/Tools/Sensors/Applications

Technologies	Examples
Wearables	Fitness trackers (vitals) Patches (respiratory, rapid changes in position/falls/balance) Small textiles (heart rate) Glasses (glucose) Watches (movement tracking, sleep) Clothing (Hexoskin®)
Health devices	Monitors (alerts, Tobii® eye tracker, glucose monitors) Smart pill and other medication adherence technology (e.g., compliance verification) Pacemakers
Phones	Smartphones (eCOA) Feature phones (text-only phones)
Mobile computers	Tablets (eCOA) Laptops Electronic clinical outcomes assessment (eCOA) devices
Media players	MP3 players (recording or uploading recordings) MP4 files

Technologies	Examples
Portable game consoles	Video games (cognitive evaluation, reflex measurement)
Navigation devices	GPS locators (geofencing, tracking hospitalizations)
Cameras	Still (dermatology or autism screening) Camcorders (audio/visual) (range of motion or gait)
Applications	General clinical trial research and electronic patient-reported outcomes Trackers (diet, fitness, diaries)
Implantables	Injectables
Patient portals	Electronic health records

Abbreviations: eCOA=electronic clinical outcomes assessment; GPS=global positioning system

4.1 Criteria for the Evaluation and Selection of mHealth Devices and Applications

mHealth Devices

The right mHealth technology for a study's needs will depend on evaluating the following criteria:

- Type and purpose of data to be collected
- Quality and frequency of data collection needed in order to meet study goals
- Reliability, maturity, and capability of the technology
- Regulations and guidances
- Participant compliance and scope of device capabilities
- Study populations
- Geographies where data collection will take place
- Budget, timelines, and support

Type of data. The type of data needed may determine the best device for the study. With "big data," think about the 5 "Vs": volume, variety, veracity, velocity, and value. Volume is the scale of the data; variety, the different types of data; veracity, the uncertainty or accuracy of the data; velocity, the timing or frequency of the data; and value, the importance of the data and its impact to the study. Frequent or continuous data streams may require a wearable or monitoring device yet can result in vast amounts of data, so the networks and systems must be capable of handling such volume. Discussions with the vendor about options for receiving the data/subsets of data/filters are key. Usability is also a factor because devices that collect significant amounts of data, such as clinically validated actigraph devices, may require data to be transmitted via cable instead of wireless Bluetooth. Internal discussions may be needed if special or additional analytics resources are required for statistical review.

Data quality. As with any data source, to ensure data quality, the device or system must be validated within the context of use. It is critical to understand the algorithms used to calculate information, especially in situations where various types of devices (e.g., tracking devices such as Fitbits) are used, or when participants use their own device. Fraud protection that verifies the participant is actually using the device should be considered. Some devices or applications may be validated for a specific purpose, setting, or domain.

Reliability. Selecting a technology with a track record of reliability is critical if the mobile data are the most important aspect of your study. If the technology has been used previously and data have been published by others, there may be evidence that it is mature and stable enough for use in clinical trials. Determining if a device has been validated within the context of use is an additional support for determining reliability. Consider the number of previous implementations inside and outside of clinical trials (e.g., wellness, healthcare) and the consistency of the data derived from these implementations. For example, blood pressure should be calculated the same across all types of technologies, and trackers should measure a step the same way. Yet devices and apps often use proprietary algorithms to calculate concepts, making it challenging to meaningfully assess how they function and compare with each other.

Newer technologies with less history of use (or use in clinical trials) may not have identified all the potential issues with the tools or may not be customizable. On the other hand, working with a new company or technology could have benefits because of the opportunity to collaborate, which may influence how data are captured and transmitted. Many healthcare device companies are eager to partner with organizations to develop solutions that can be integrated within broader systems. It is important to verify that the technology can capture and transmit data reliably, equivalently, securely, and privately.

Regulatory. Data managers need to understand the continually evolving regulatory landscape when selecting an mHealth technology (see Section 8). If you are planning to use a new device, wearable, or technology in your program, it is advisable to discuss it with the applicable regulatory agencies to ensure the method of data collection is acceptable. There are also country-specific regulations that have to be met for use of mHealth devices or use of them in specific settings. For example, there are countries where mHealth devices can only collect data if the participant is in a healthcare environment.

Compliance and capabilities. Part of data quality includes proper compliance with device use and device capabilities in various environments. Devices should have the ability to assist with user compliance and engagement via a companion application by implementing features such as alerts to remind them to submit data or use the device. Online technologies associated with central monitoring, with quick feedback to the sites, can significantly reduce missing data. Capabilities should include the ability to monitor when the device is not in use, when a participant is not wearing the device properly, or is using it in otherwise noncompliant ways. Device infrastructure capabilities are critical to ensuring that data can be collected in various settings related to connectivity, power, and system stability. When data are to be continuously uploaded onto a server or cloud, then contingency plans should be implemented if connectivity is lost for some period of time due to power loss or if a participant is out of the service area.

Study population. The device should meet the needs of the population in regard to age, gender, or physical capabilities. Older study participants may require devices with different accessibility requirements, (i.e., larger text, size of buttons, size of screens, color and contrast of screens). Or, they may not have access to devices. Users with conditions that limit their dexterity need devices that can accommodate their needs. Usability testing in addition to validation should be conducted to ensure user interfaces and screens are designed to perform the tasks expected for the study population.

Geography and environment. Medical devices might need approvals in specific regions or require clinical trial waivers if used in a trial. Participants need local language manuals and user interfaces. Certain areas of the country or world may not have the highest speed of transmission or access to wireless services, so data volume or frequency should be considered if wireless or cellular service is limited. Also consider whether real-time data transmission is a possibility or if the data are stored on a device and transmitted at certain timeframes. “White coat syndrome” may be an issue when it comes to heart rate measurements from fitness trackers. Also, there may be environments where heart rates are higher or lower because of what the participant does while wearing the device (e.g., fireman vs. librarian.)

Technologies such as smartwatches that use Bluetooth may introduce challenges related to poor cellular service, different frequencies, and battery life in certain contexts. Smartwatches, smartphones, and other devices may require frequent charging, which may not be possible in places with unreliable electricity sources such as rural or remote areas. The type of energy source, such as rechargeable, replaceable, or solar, needs to be evaluated. To avoid situations where data interruption or data loss could occur, consider proactively addressing these issues in the study protocol, statistical analysis plan, and data monitoring plan.

Budget, timelines, and support. When selecting a device or technology, decisions should be based not only on budgets at initial purchase and implementation but also on maintenance and support needs over time. Technologies and their infrastructure change rapidly and may impact the capabilities. Newer software and application versions may not work as well on older technology. Support from the vendors will be more crucial to maintain systems and respond to issues due to hardware and software.

mHealth Applications

The proliferation of mHealth-related apps is due to the interest in the opportunity to track patient information in real time. Data managers and informaticists should understand the development process, usability, maintenance plan, and data quality of such apps. When developing apps for mobile devices, developers have a choice between native and hybrid apps. Knowing the different characteristics of the two types of apps is important because the type of app can impact resources, device and targeted participant populations.

Native apps. Native mobile apps are developed using the programming language specific to the platform, such as Objective C or Swift for iOS, Java for Android operating systems, and .NET languages for Windows Mobile. (The majority of device users will have iOS or Android devices.) However, because native apps execute only on the platform for which they are written, there may be a need to develop and maintain multiple applications for use on each platform. Native apps are installed directly on the device, which provides better speed and ease of data collection and may aid in the retention of study participants by reducing frustration with network connectivity issues and load time. Native apps also allow for the opportunity to integrate with features of the mobile device (e.g., camera, voice recorder, and geographical location). Data stored for these apps are restricted to what is required per protocol.[13]

Hybrid apps. Hybrid mobile apps are cross-platform compatible and can perform the same functions as native applications but may have some limitations when accessing the device’s hardware. Hybrid mobile frameworks like PhoneGap, Ionic, Titanium, Xamarin, etc., are good for developers with experience in common open-source programming languages. Hybrid apps work well in situations where Bring Your Own

Device (BYOD) is allowed. For example, PhoneGap, which uses standard web programming languages to develop the core of the application, also provides additional libraries for developers to use when there is a need to access the resources of the native operating system.

Clinical research projects using apps programmed for a specific platform will often need to support more than one mobile operating system, version, and device. This situation might require some relaxation in validation requirements because it would be prohibitive to fully validate the app on each platform and version. Creating mHealth apps for multiple platforms allows more users to participate in the study and allows them to change devices without dropping out—both critical to long-term follow up. Yet there remain challenges with ensuring ease of movement from one device to another, and with the comparability of data collected across different devices.

Further mHealth App Considerations

Evaluating and selecting the right mHealth app also involves these considerations:

Experience and technical aptitude. Web-based apps can be updated centrally without interruption to study participants, but may limit their ability to use specific functions. While native apps have full access to all features of the device, the end-user will be required to download any updates. The choice of technology also depends on the skillset of the development team. It will ease the transition to mHealth technologies if the developers have experience with the programming languages the platform needs.

Measurement tools and validation. Standard questionnaires, scales, and other measurement tools should be validated for the various platforms. Prior to converting standard scales to an electronic format, the author of the scale should be consulted to ensure that the scale is not made invalid when used on an electronic platform and/or psychometric validation. Some licensed scales require written permission to convert from paper to electronic format or provide specifications on how the electronic version should be presented. There also may be a need to explore the effect of different display sizes and resolutions on the way patients respond to validated scales. After these tools have been validated, they could be ready to implement in studies with minimal delay. There may also be a need to prove equivalency across all the variations used within a study or submission.

Usability. Mobile apps should be developed with usability in mind. Most data managers are familiar with user acceptance testing, but they should also perform usability testing. Usability testing ensures the user can perform the actions and tasks expected without complication. Apps that may be challenging or require significant training may both reduce compliance to the trial protocol and lead to poor data quality.

Maintenance. Because technology is rapidly changing, a maintenance plan will be needed for longer studies to keep applications in sync with newer technologies and devices and still accommodate users who may not immediately upgrade their device. Updates should be considered whenever a new version or patch is released to the operating system. Security updates are often considered mandatory and should be part of the maintenance plan. This will minimize interruptions to users. Carefully consider who is responsible for creating this plan. If the responsibility is outsourced, the sponsor should ensure the plan meets their needs in the event the relationship with the third-party company terminates before execution of the plan.

Long-term costs. When planning the support of mobile apps, study teams should plan budgets that cover the life of the app for support, upgrades, maintenance fixes, and any other factors that could impact the app.

Automatic data capture. Identify ways to incorporate data captured by the device programmatically instead of requiring input from the user. For example, when using a mobile app to capture step information, the developer should pull data via integration with the wearable's application programming interface (API) instead of requiring the user to enter the data manually. In some clinical apps, this will require industry data and exchange standards to ensure data quality.

Data quality. Steps should be incorporated to ensure data completion, reliability, and accuracy when designing and implementing apps. Built-in alerts that remind users to complete and/or submit data are useful as long as they do not cause alert fatigue or allow the user to reconfigure the alerts. Special attention should be given to accurate date and timestamps of measurement data. It is recommended to synchronize date and time of the device with a reliable time source regularly. The traditional query and source data verification process will significantly change for many aspects of the clinical trial process with the use of mHealth technologies. This will mean that apps need to be designed with a focus on quality balanced with ease of use. See Section 6 (People and Process) for further information on changes to roles and responsibilities in assessing quality.

4.2 Device Provisioning Models

After making the decision to use a particular mHealth technology in the clinical study, the question moves to implementing and provisioning the devices. Broadly speaking, there are three distinct ways to provision the devices.[14]

1. A 100% centrally provisioned model in which all users are provided the same device. This is the model most used in eCOA settings.
2. A 100% bring-your-own-device (BYOD) model in which all users provide their own device. This model requires that participants have a particular mobile device, and it may not be practical for global trials.
3. A combination of the two models involving partial provisioning and partial BYOD. This model is practical for global trials.

Trial-specific needs should drive the decision-making for implementation. In **Tables 4-6**, we list some examples of the pros and cons of each provisioning model. We do not describe mixed data collection (the use of devices for some users but not others) as its use is not recommended. Additional provisioning considerations are in Section 5 (Managing Study Risk).

Table 4. Model 1: 100% Centrally Provisioned

Pros	Cons
• Allows for uniform data collection • Variability in device models, size, etc., between users is eliminated and same device is used for the duration of trial • Process of equivalence testing, if required, is simple and well understood • Device support via one central helpdesk • Consistent device and uniform design allows simpler training plans • Current eCOA vendors are most experienced in this type of implementation • Ensures compatibility with other connected devices • Precedents for acceptance of data submitted to regulatory agencies	• Most expensive • Potential increase in user burden as those who already have a similar mobile device now need to remember to carry and keep an extra device charged • Increase in site burden as the management of device inventory resides at the site • Higher risk of potentially outdated devices in case of long-term trials • Implementation of a device replacement plan is required

Table 5. Model 2: 100% Bring Your Own Device (BYOD)

Pros	Cons
• Potential cost savings as BYOD costs are focused primarily on software and not software plus hardware • Alleviates burden of carrying multiple devices • Users are likely to keep the devices charged and with them at all times • Alleviates site burden; no device inventory management needed • Lower maintenance and logistics effort • Only trial-focused training required as users are already familiar with their own mobile devices and features such as on/off, screen advance, and charging procedures; could potentially increase compliance • User devices may not be compatible with the current technology infrastructure	• Potential of screen-rendering flaws on varying screen sizes (in a traditional eCOA setting) • Not all users may have the mobile device required for the clinical trial, which may impact enrollment • Users may accidentally or purposely delete the app on their own mobile device, resulting in data loss; requires robust data monitoring plan to catch this as close to the event as possible • Lack of control over alarms and reminders • More prone to malware and data corruption if device is not kept updated with the latest operating system • If an excessive amount of data are transmitted, sites and participants may require sponsor to develop ways to reimburse or share cost of wireless data plans • Potential incompatibility with other connected devices (e.g., glucometer or blood pressure monitor) • Uncertainty on equivalence between data collected from multiple devices in case of data being submitted to a regulatory agency • Uncertainty about how the mHealth technology will work when upgraded to the latest operating system • Technical support needs to be knowledgeable of the varying mHealth technologies allowed in the clinical trial • Not all users may have the mobile device required for the clinical trial; a full BYOD model might result in selection bias and a

Pros	Cons
	non-representative sample of the patient population • Higher opportunity for patients to get distracted during logging assessments by text messages, phone call, etc. • Providing training and support for the wide range of devices that might be seen in a study

Table 6. Model 3: Mix of Centrally Provisioned and BYOD

Pros	Cons
• User-centric • Allows inclusion of those who may not have a mobile device at all or one that is incompatible with the trial needs • Lowers site burden • Potential lower cost than 100% central provisioning	• Increases complexity with the mix of two approaches • Same disadvantages as BYOD and 100% provisioning

4.3 Implementation Challenges of BYOD Devices

Organizations considering a BYOD model (100% or mixed) should be aware of the following implementation challenges and proactively develop plans to address them:

- *Copyright owner agreement.* Before implementing copyrighted material in any device, ensure the copyright owner agreement is obtained. If data are to be used for primary or secondary endpoints or a label claim,[15] the sponsor will need to discuss with regulators any requirements for demonstrating equivalence across the range of devices within the study. Regulations may also require registration of certain types of devices classified as "medical devices."[7] The device or combination of devices implemented needs to be evaluated to determine if they fit these criteria. When considering the use of mHealth devices and services, the sponsor should understand the nature of the tools being used and discuss the methodologies and data capture devices with the applicable review divisions in advance. For further information, see Section 8 (Regulatory Landscape).

- *End-to-end data flow.* Selecting a data collection modality and its implementation approach cannot be successful without defining and understanding the end-to-end data flow. The data management plan or other data-handling document should describe the data flow from data collection to third-party hosting servers to the sponsor's clinical database.[1] Some mHealth technologies, by design, may stream continuous data to their servers (e.g., vitals monitoring, activity monitors) more frequently, thereby generating more data than required per the protocol. In these cases, it is critical to prospectively document how the data will be natively collected and which parts or intervals of the data will be brought into the clinical database.

- *Training and helpdesk.* In the event that users have trouble entering data into their own device, they may be tempted to call their phone/data provider for issues that may have to do with the application (e.g., eCOA), or they may reach out to the application provider for issues that may have to do with their own hardware or data connection. A robust training plan addressing these specific logistical issues is recommended.

- *Protected health information (PHI).* Users who store PHI on their devices should also be trained in securing their devices appropriately, such as requiring a PIN or biometric authentication.
- *Backup plan.* Irrespective of a full or mixed BYOD approach, we recommend that sponsors, in alignment with their clinical sites, develop a robust backup plan for cases when a user's device is lost or stolen so that clinical data collection remains as uninterrupted as possible. Backup plans should consider, for example, switching the provisioning model if a new device needs to be provisioned due to damage or loss, or if the participant chooses to use his or her own device after having been provisioned one.
- *Robust data monitoring plan.* The close monitoring of data as it is being collected is another key to success and will help avoid costly workarounds later. Front-end or on-screen edit checks or prompts may be able to be built into the mHealth device to assist with data monitoring.

4.4 Transmission Methods

Transmission methods for mHealth devices continue to evolve, connecting devices in various ways including:

- Cellular networks: 2G, 3G, 4G, LTE
- Wireless local area network (WLAN): Wi-Fi (802.11x)
- Wireless personal area network (WPAN) or wireless sensor actor networks (WSAN): Bluetooth, ANT, ZigBee, radiofrequency identification (RFID)
- Line-of-sight: Infrared (IR) technology

The type of connection should match the intended use of the device. Each connection type has a different data transmission range, data throughput, and power management need. Physical location in the user's home can affect data transmissions, as can interference from other devices. The device should be evaluated to ensure that the signals will communicate reliably with their upstream connection.

Data transmission may occur in different configurations; for example, a remote model may be used where data are pushed to another location (i.e., cloud server), or a local model may be used where the data are stored on the device until retrieved. It may be best to have a hybrid methodology available, where the data are stored locally until pushed to a remote location. The security of transmission and data storage (both remote and local), the protection of privacy, and ensuring data integrity all need to be carefully considered in a clinical study.

4.5 Data Chain of Custody: Traceability

In the eSource white paper,[1] Principle 6, Control for Quality, explains that tracking, tracing, and documenting the flow of data from generation to storage is one of the most critical steps when evaluating and selecting any type of technology. This activity involves establishing the data chain of custody (e.g., understanding how the data are generated), how the data are connected to other devices or networks, and who has access to the data after it is generated and stored on a device or server before it reaches the data management team. If the study team is working with a vendor or communication company, there should be discussion and documentation on how the data are temporarily or permanently stored, who has access to it, and all logical/physical controls. It is also key to determine, contractually, who has ownership and rights to data use. Identifying and validating data transformation procedures from the point of collection through the data's lifecycle should be documented because it can affect the data quality and reliability. The final copy of the data should include the device serial number and original device timestamp of collection in the audit trail so that the data may be linked to calibration records for the device. This will allow for automated source data verification (SDV) of those records.

5. Managing Study Risk

We believe that mHealth technologies will improve the clinical trial and research process, but as with any data collection method, there are potential business risks related to tools, processes, or data collected from study participants.[16-18] Identifying such risks and evaluating their likelihood and impact will influence the type of risk mitigation plan needed by the study team. In addition to the typical risks that are encountered during a clinical trial, mHealth technologies may introduce some different challenges. We encourage teams to consider the examples in **Table 6** while evaluating their risk plan.

Table 6. Potential Risks of mHealth Technologies

Risk	Implication/Impact	Possible Mitigation Strategy
Lack of adequate public or private access to technology, web, wireless data plans, or network coverage	Limit populations in clinical trials and studies, inequality in access to clinical trials, low or slow enrollment; bias in clinical analysis; Enrollment of a patient who is unable to participate	• Supply devices • Provide phone cards • Lower the barrier to obtain devices and plans • Allow BYOD • Compatibility check of the BYOD device • Create a Participant Characteristic Assessment Plan for mHealth to understand the patient population's constraints, capabilities, local or country restrictions, and/or willingness to use mHealth
Consistent /adequate validation or calibration of devices	Inconsistent or variation in data	• Validate applications and tools in various types of situations • Implement regular processes for calibration and trend analysis • Get raw data
Too many apps asking for user's direct entry in a protocol; user burnout and compliance wanes	Poor data quality and decreased data completion	• Identify other methods for data collection that collect data passively (e.g., certain types of wearables) • Find ways to keep user engaged

Risk	Implication/Impact	Possible Mitigation Strategy
Loss of privacy or user's perceived risk of loss of privacy	Difficulty in IRB approvals and participant enrollment	• Establish data chain of custody in contracts • Establish controls over access and minimize data stored on device • Establish data chain of custody in contracts • Establish controls over access and minimize data stored on device • Update informed consents to address general privacy concerns and outline how and where these data will be used. Users should be able to opt out of secondary uses of data that are beyond the primary goal of the protocol. This should alleviate some of the IRB/EC worries and not delay approvals.
Attributability	Device use by someone other than the consented study participant has an impact on data analysis	• Ensure password or biometric verification to open or submit data or alerts when device is removed • Provide centralized statistical analytics that use baseline and comparative algorithms to detect if someone other than the user is using (or wearing) the mHealth device
Technology interruptions	Users lose or break the device; phones are hacked; differences in countries, wireless data plans, billing; plan terminated; service outage; data limit reached	• Based on population and geographic location, create a back-up provisioning plan (i.e., provide devices or cards for additional text messages). Mixing modalities, especially a combination of paper and electronic, requires additional strategies

6. People and Processes

The strategic and tactical decisions regarding the use and adoption of mHealth technologies can be challenging for study sponsors. At the forefront of the decision-making process are people with new skillsets and knowledge of processes who are tasked with determining the right approach for the operational use of mHealth and eSource. To enable effective strategic decision-making around mHealth technologies, sponsors should foster in their staff the expansion of learning and experience. Awareness of eSource-specific regulatory guidance, global regulations, and current thinking in the field is critical to the implementation of mHealth technologies throughout the life of the clinical trial.

With mHealth, the data manager's role now becomes one of expert in eSource data collection and management. Differences in data collection methods (user-entered vs. automatic) requires an understanding of study needs. Acquiring mHealth expertise is instrumental in all aspects of the trial: vendor/device selection, protocol design, device design, database build, trial execution, training, monitoring, device inventory management, privacy, security, data hosting, data transmission, data storage, and data integration as well as in the traditional tasks of data reporting, data review, and analysis. The data manager is a key contributor and coordinator of mHealth activities, directing other roles in IT, statistics, sourcing, and trial/site management.

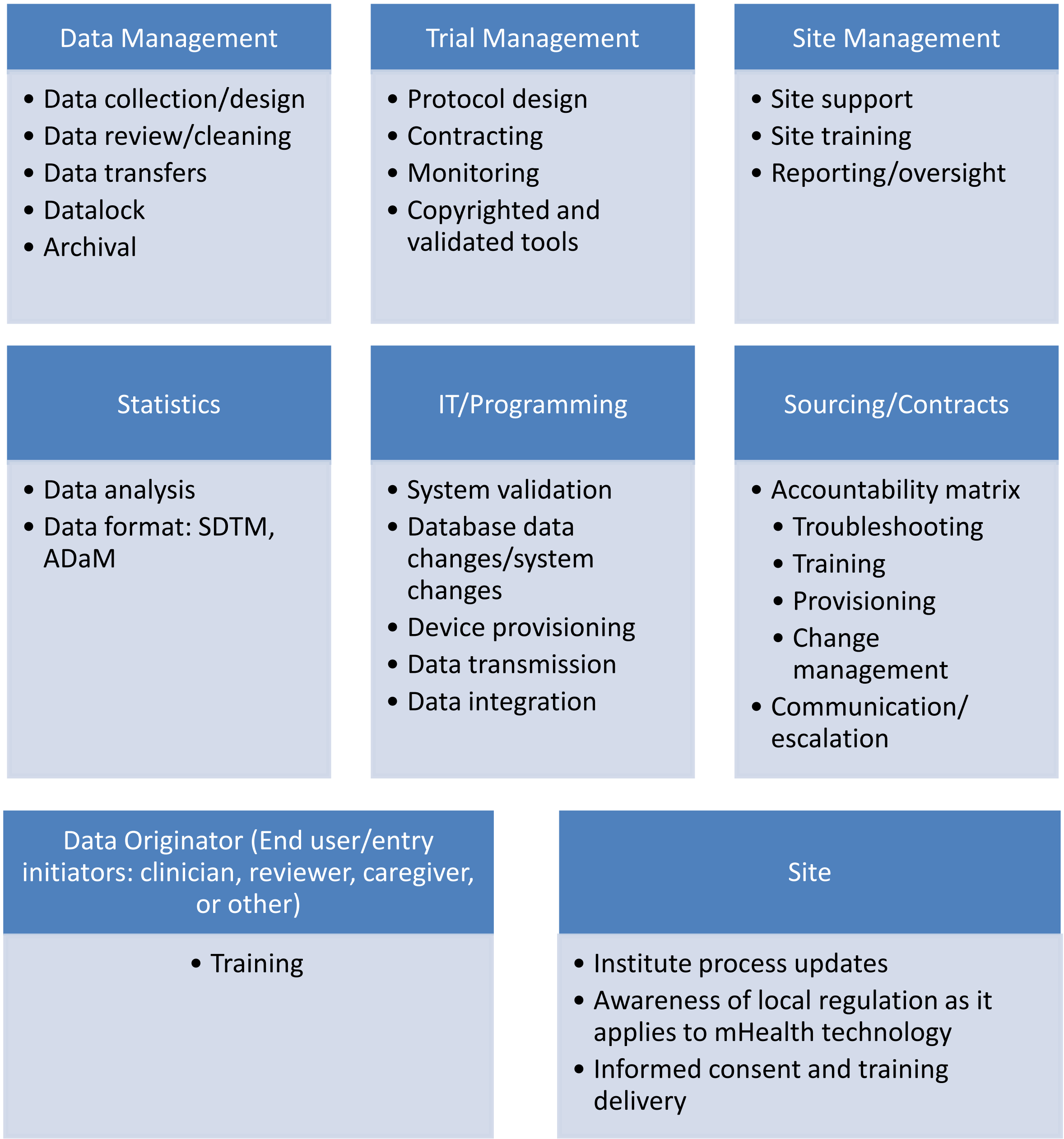
6.1 The Seven Principles of eSource

The seven principles from the SCDM eSource white paper[1] apply to all aspects of the clinical trial and are key to successful mHealth implementation:

1. Use solutions that are fit for purpose
2. Declare the source
3. Capture data when first generated
4. Control electronic data
5. Leverage automated quality checks
6. Control for quality
7. Conform to regulations and guidelines

Applying these principles to trial activities requires adjustments to roles, responsibilities, policies, and processes. We suggest that data managers, as mHealth experts, lead a cross-functional team to create a guiding structure for the handling of mHealth data. While the decision to use a particular mHealth technology may not rest with data managers, they should facilitate communication and ensure that the technology meets regulatory requirements and statistical rigor. **Figure 1** lists important activities to evaluate and possibly modify for each function supporting the successful deployment and conduct of eSource and mHealth technologies.

Figure 1. Activities and Tasks to be Assessed and Modified for mHealth Implementation



Data Management

- Data collection/design
- Data review/cleaning
- Data transfers
- Datalock
- Archival

Trial Management

- Protocol design
- Contracting
- Monitoring
- Copyrighted and validated tools

Site Management

- Site support
- Site training
- Reporting/oversight

Statistics

- Data analysis
- Data format: SDTM, ADaM

IT/Programming

- System validation
- Database data changes/system changes
- Device provisioning
- Data transmission
- Data integration

Sourcing/Contracts

- Accountability matrix
  - Troubleshooting
  - Training
  - Provisioning
  - Change management
- Communication/ escalation

Data Originator (End user/entry initiators: clinician, reviewer, caregiver, or other)

- Training

Site

- Institute process updates
- Awareness of local regulation as it applies to mHealth technology
- Informed consent and training delivery

6.2 Expanded Roles and New Mindsets

The role of data managers will expand as other functions depend on them for information about methods of collecting fit-for-purpose data and for understanding the data chain of custody. A new mindset is needed by data management to define data review and data-cleaning processes. In the mHealth era, activities related to eCRFs, transcribed data entry, and query-to-site interactions are replaced by tasks related to patient-reported data, site or third-party transfers, queries for completeness instead of content, reporting to evaluate safety signals, and trend analyses to identify potential abnormalities within the dataset. Data integrity checks look for compliance (e.g., did the user wear the actigraphy watch?), completeness (e.g., are all records accounted for?), and potential device malfunctions (e.g., are the data being reported incompatible with reality?). The device is the *only* data source, and these data cannot be queried. Data locks, snapshots, and extractions become more streamlined as the evaluation of mHealth data is in real time and focuses on metadata header reconciliation and completeness instead of content. **Table 7** describes the types of interactions between data managers and other functions that are critical to the successful implementation of mHealth in clinical trials.

Table 7. Data Management Interactions with Other Roles and Functions

Role/Function	Interaction
Clinical programmers	Establish appropriate controls for hosting, maintenance of device operating software, processes for data transfers and/or direct integrations with a data warehouse. Archive of the user's eSource data needs to follow a clear data chain of custody from the user to the end to ensure its integrity and traceability.
Archivists	Follow guidance from the SCDM eSource white paper.[1] The archived data and the supporting documentation should tell the data story from the study participant through archival.
Statisticians	Adjust statistical methodologies to accommodate large volumes of data from continuous data collection and to establish appropriate error rates based on cleanliness of data. The reduced ability to query the data will result in more real-life data, which has its own implications for analysis (e.g., how to handle missing data, unexpected data, or conflicting data). Working with data managers, statisticians will define appropriate reporting and tools for trend analysis. Also they will provide key inputs into the dataset format (e.g., SDTM or SAS for reported or raw data, ADaM for analysis) and what type of information must be collected to support analysis. The whole process should ensure (by statistically sound means) that bias is avoided.
Global vendor sourcing managers	Assess the vendor landscape for experience, capabilities, and services provided. Sourcing should ensure the vendor's contracts align with eSource principles and that there are clear lines of accountability to protect the eSource's data integrity and traceability. The essential rule in any eSource collection is that the sponsor/contract research organization is not in control of the site's data (Principle 4) and at no time amends the data without the patient's consent.
Quality assurance auditors	Be aware of how the data are collected, transferred, and stored in order to assess compliance.
Regulatory associates	Provide directional input on compliance factors of mHealth and eSource including new country regulations, security considerations, and back-up/archival procedures as developed by the regulatory agencies.
Clinical site management	Do not assume a certain level of user understanding of the technology; understanding cannot be ambiguous. It is recommended to run simulations of user training and training materials to determine if they are complete, clear, relatable, and engaging.

Role/Function	Interaction
Staff and user training	Typical training provided to medical staff at a site will most likely be inadequate for a study participant. Consider engaging usability experts, site staff, or clinical research assistants (CRAs) to assist with user-friendly or site-friendly designs that will help increase data quality and promote reliable data collection. Ensure that the protocol incorporates the use of the mobile technology into its design since afterthoughts create multiple challenges. During trial execution, provide monitoring or activity reports so that the CRAs can oversee the progress at the site and verify device compliance by the users. Quick actions to provide additional helpdesk, or other support or training are key in providing a good experience as well as high-quality data. Sites need to understand how the device collects and transmits the required data, and how sites will maintain control and access to meet their responsibilities in maintaining adequate case histories. They must support the methods and engage with the users in their training.

As use of technology becomes more frequent—and more global—roles and responsibilities will continue to evolve in conjunction with the management and execution of studies using mHealth. New skills of a data manager will include:

- *Deep knowledge of data.* Knowledgeable in the characteristics of different types of data, such as EHR data from inpatient vs. outpatient from a biorepository. Understanding the implications of data context, quality, source, amount, and workflow.
- *Data integration*. Knowing the integration points of data. Data flowcharting skills are helpful in this analysis.[19]
- *Data profiling.* Understanding completeness, quality, and age of data.
- *Analysis.* Using technology to identify and read anomalies and understand their impact on the total study.
- *Entity resolution.* Knowing for certain it is the same user when gathering data from multiple sources.
- *Awareness and curiosity.* With a rapidly changing environment, staying aware of the latest issues, standards, and regulatory requirements.
- *Proper documentation.* Within the informed consent process, study participants must be informed of the importance of the data being collected and preserve the confidentiality, retention (e.g., uninstalling the app), and integrity of the data. This behavior is especially important in BYOD where proper app and data controls may not exist.

7. Standards for mHealth

It is important with the increased use of technology to implement seamless integration between applications, devices, and systems that collect and exchange quality user information. Standards are a foundational element for enabling true interoperability. While there are certain standards associated with mHealth technologies, the focus has not been on data exchange until now. The most mature standards are in the web application and healthcare device field where the Worldwide Web Consortium (W3C) and ISO standards are used.[20] Standards organizations such as Health Level 7 (HL7) and the Institute of Electrical and Electronics Engineers (IEEE) are identifying gaps and working toward modifying existing or developing new standards to address application development, data exchange, communication protocols and devices (see the Appendix, Mobile Standards to Facilitate Data Collection, Exchange, and Security).

The healthcare and research industries are heavily focused on developing standards and governance around the exchange of data between the consumer and the researcher or health entity; exchange of data between applications; security of applications, devices and data; methods of exchange; policies for data ownership; and other infrastructure support. Of the many standards in use today, we describe (1) exchange or transmission standards, (2) content standards, and (3) security, interoperability, and privacy standards.

7.1 Exchange or Transmissions Standards

Exchange or transmission standards focus on standard protocols for sending and receiving data that reduce the overhead of custom integration between systems. For example, most researchers are familiar with transmission standards such as the Clinical Data Interchange Standards Consortium's (CDISC's) Operational Data Model. The HL7 Fast Healthcare Interoperability Resource known as FHIR (pronounced "fire")[11] is one of the newest for exchanging information between systems, specifically mHealth systems with API content. There remains a need for other exchange standards, such as common APIs, standard exchange messages, and data standards. These types of standards will facilitate linkage from multiple sources, ease data aggregation, and enforce security.

7.2 Content Standards

Content standards usually define the semantic information such as the data fields or terminology. Examples of content standards include the International Statistical Classification of Diseases and Related Health Problems ICD-9 or ICD-10, HL7, Therapeutic Area Standards, and CDISC's Study Data Tabulation Model (SDTM) and CDASH. Content standards can also facilitate consistent data collection across applications and devices for those who want to use BYOD models and also facilitate sharing between EHR/EMR and clinical trial databases.

7.3 Security, Interoperability, and Privacy Standards

Several major standards development organizations are collaborating to support data integration. In addition to exchange and interoperability, they are also targeting standards and policies to support security and data ownership. For example, consumers participating in clinical studies may not be aware that their data are flowing over public networks (the internet or cellular networks), where no contractual or data use agreements are in place. This means that the wireless or technology company could access and use their data without any accountability.

Standards are also needed to describe the security of the data in short messages (e.g., text, Twitter) while in the possession of a third-party vendor and to ensure that the data are generated by the individual in an expected format for streamlining data exchange. The researcher likely has little control over how these data are secured, but the risks should be made clear to the study participant via informed consent.

From a privacy perspective, when using devices that collect more data than is consented to for research (e.g., a smartwatch that collects your location, heart rate, IP address), it is key to ensure in the contract and in the data flow that the technology vendor can provide the sponsor copies of only consented-to data. The same holds true for using an application and hosting of the data that includes other personal metadata.

Currently, there are concerns to be addressed around the security of short messaging, data that pass through third-party party vendors, and ownership of data. The standards development organizations are in the process of adapting current standards to mobile and wearable technologies but also must create standards that deal with these new challenges to promote interoperability while maintaining security and privacy.

More work is needed to determine what standards are necessary, and because healthcare personnel and researchers are stakeholders with many of the same goals, they should work together to develop the standards to make it easier for users to provide information. There is opportunity now for further collaboration among healthcare, research, and patient communities. Rather than working in silos, we encourage these groups to work together to identify and develop standards for the collection, exchange, and quality of data specific to mHealth technologies.

8. Regulatory Landscape

Principle 7 of SCDM's eSource white paper[1] underscores the importance of conforming to applicable regulations and guidelines. The rigorous science relevant to all data collection methodologies should also be reflected in regulations and guidances specific to mHealth and eSource. Data managers should be aware that guidances are revised and updated often, so it is always good practice to check for the most recent publications before starting any study.

8.1 Safe Harbor Framework

Mobile health devices, applications, and the entire data chain of custody must take privacy and security requirements into account and adhere to local regulations and laws (e.g., HIPAA, EU 2002/58/EC ePrivacy). While the United States and the European Union have their own privacy laws and directives, "in order to bridge these differences in approach [to privacy] and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a 'Safe Harbor' framework."[21] However, on October 6, 2015, the European Court of Justice issued an advisory regarding the "adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce."[21] Because the situation with safe harbor continues to evolve, consultation between your company's legal department and the EU data protection Article 29 working party is appropriate.

8.2 Regulations and Guidances Applicable to Use of mHealth Technologies and eSource

Any mHealth device (e.g., smartphone), wearable device (e.g., Fitbit), mobile app, or data/storage/communication system must be assessed to determine if it qualifies as a medical device under section 201(h) of the Food, Drug and Cosmetic Act (FD&C Act), with additional examples and clarifications under the corresponding FDA guidance.[6] If it does qualify, then regulations under FDA's Center for Device and Radiologic Health (CDRH) must be followed.[7,15] These include 21 CFR Parts 807, 808, 812, 820, and 880. The EU Directive 90/385/EEC regarding active implantable medical devices (AIMD), Directive 93/42/EEC regarding medical devices (MDD), or Directive 98/79/EC regarding *in vitro* diagnostic medical devices (IVDD) need to be adhered to and are requirements for obtaining the CE mark.[22]

Note that FDA's oversight is based on the functionality of the device—not the platform. For all activities involving the use of computerized systems to create, modify, maintain, archive, retrieve, or transmit clinical data to the FDA, computer system validation of the device/software is required as described in 21 CFR Part 11[23] and in the FDA guidance on computerized systems used in clinical investigations.[24] For the EU, the electronic signatures directive applies.[25]

Per the Mobile Medical Applications guidance, "the FDA strongly recommends that manufacturers of all mobile apps that may meet the definition of a device follow the Quality System regulation 21 CFR 820 (which includes good manufacturing practices) in the design and development of their mobile medical apps and initiate prompt corrections to their mobile medical apps, when appropriate, to prevent patient and user harm."[6,7] For patient-reported outcomes, FDA guidance reiterates the need to follow existing guidance for computerized systems and also states expectations for eSource.[15,26]

Investigators participating in clinical trials and using eSource for patient charting (e.g., EHRs) are expected to follow the retention requirements outlined in ICH E6 Section 8[27] and FDA 21 CFR Part 314 and Part 312 regulations.[19] Sites using eSource must understand the data flow and how it meets the FDA 21 CFR Part 312.62(b) obligations of maintaining case histories under this data flow. Further guidance on expectations for sites and study sponsors related to eSource are in CDISC's eSDI white paper,[28] FDA's Electronic Source Data in Clinical Investigations,[29] and the EU's reflection paper on expectations for electronic source data.[30]

Ask the FDA for a meeting to discuss novel or new data collection methods and include the Office of Scientific Investigations (OSI).[31] At this meeting, bring your technology vendor to help explain the data flow and data collection, storage, and transmission. If your study uses BYOD, discuss requirements and methods for demonstrating equivalence.

9. Conclusion

Just as electronic data capture has had a profound impact on the way data are collected and managed within clinical trials, mHealth and eSource are driving technological advancements in data collection while providing a benefit directly to clinical study participants. Mobile health technologies are enabling broader user participation from different geographies and in different trial types, new patient-centric study designs, early symptom detection supporting adaptive design goals, and increased ease in collecting real-time data. To help with the effective adoption of mHealth technologies as new electronic data sources, we presented a principles-based approach to the evaluation of the impacts of eSource on technology, people, processes, standards, and regulatory requirements. Data managers—as experts in data source, data flow, and data collection—will see their roles expand and should be positioned to drive the process changes necessary for successful adoption of mHealth technology across the clinical trials landscape.

10. References

1. Society for Clinical Data Management (SCDM). eSource Implementation in Clinical Research: A Data Management Perspective. June 2014. Available at: http://www.scdm.org/sitecore/content/be-bruga/scdm/Publications.aspx. Accessed November 5, 2015.

2. U.S. Department of Health and Human Services. Health Resources and Services Adminstration (HSRA). Health Information Technology and Quality Improvement.

mHealth. Available at: http://www.hrsa.aquilentprojects.com/healthit/mhealth.html. Accessed November 5, 2015.

3. National Institutes of Health. NIH supports development of a mobile health research platform, Available at: https://www.nibib.nih.gov/news-events/newsroom/nih-supports-development-mobile-health-research-platform. Accessed July 22, 2016.

4. National Institutes of Health. Privacy and Security in Mobile Health (mHealth) Research. Available at: http://www.arcr.niaaa.nih.gov/arcr/arcr361/article14.htm. Accessed August 22, 2016.

5. National Institutes of Health. mHealth - Mobile Health Technologies. Available at: https://obssr-archive.od.nih.gov/scientific_areas/methodology/mhealth/index.aspx. Accessed August 22, 2016.

6. U.S. Food and Drug Administration (FDA). Mobile Medical Applications. Available at: http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm. Accessed July 25, 2016.

7. U.S. Food and Drug Administration (FDA). Center for Devices and Radiological Health and Center for Biologics Evaluation and Research. Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff. Available at: http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm263366.pdf. Accessed November 5, 2015.

8. MIT Technology Review. Apple and IBM's Plan to Make Smarter Health-Tracking iPhone Apps. April 22, 2015. Available at: https://www.technologyreview.com/s/536846/apple-and-ibms-plan-to-make-smarter-health-tracking-iphone-apps/. Accessed July 25, 2016.

9. Apple Inc. Develop health and fitness apps that work together. Available at: https://developer.apple.com/healthkit/. Accessed July 25, 2016.

10. Apple Inc. Health apps. Available at: http://www.apple.com/ios/health/. Accessed July 25, 2016.

11. Fast Healthcare Interoperability Resources (FHIR). Fast Healthcare Interoperability Resources (FHIR) Specification. Available at: https://www.hl7.org/fhir/overview.html. Accessed July 28, 2016.

12. Google. Health and fitness apps. Available at: https://play.google.com/store/apps/category/HEALTH_AND_FITNESS?hl=en. Accessed July 25, 2016.

13. Technopedia. Native mobile app. Available at: https://www.techopedia.com/definition/27568/native-mobile-app. Accessed November 5, 2015.

14. Coons SJ, Eremenco S, Lundy JJ, O'Donohoe P, O'Gorman H, Malizia W. Capturing Patient-Reported Outcome (PRO) Data Electronically: The Past, Present, and Promise of ePRO Measurement in Clinical Trials. Patient. 2015;8(4):301-309. PMID:25300613. doi:10.1007/s40271-014-0090-z.

15. U.S. Food and Drug Administration (FDA). Center for Drug Evaluation and Research (CDER), Center for Biologics Evaluation and Research (CBER), and Center for Devices and Radiological Health (CDRH). Guidance for Industry: Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims. Available at: http://www.fda.gov/downloads/Drugs/.../Guidances/UCM193282.pdf. Accessed November 5, 2015.

16. AppBrain. Top ten Google Play categories. Available at: http://www.appbrain.com/stats/android-market-app-categories. Accessed July 26, 2016.

17. Intersog. State of mHealth Apps Development Market 2014. Available at: http://intersog.com/blog/state-of-mhealth-apps-development-market-2014/. Accessed November 5, 2015.

18. Luden I. Gartner: Device Shipments Break 2.4B Units In 2014, Tablets To Overtake PC Sales In 2015. Available at: https://techcrunch.com/2014/07/06/gartner-device-shipments-break-2-4b-units-in-2014-tablets-to-overtake-pc-sales-in-2015/. Accessed July 26, 2015.

19. U.S. Food and Drug Administration (FDA). Code of Federal Regulations. 21 CFR Part 312. Available at: http://www.ecfr.gov/cgi-bin/text-idx?SID=bfa365055d6b5b5384bd5f1f31141494&mc=true&node=pt21.5.312&rgn=div5. Accessed July 27, 2016.

20. W3C. Standards for web applications on mobile: current state and roadmap. August 2015. Available at: http://www.w3.org/Mobile/mobile-web-app-state/. Accessed November 5, 2015.

21. Export.gov. Safe harbor frameworks. Available at: http://www.export.gov/safeharbor/. Accessed November 5, 2015.

22. European Commission. Medical devices. Available at: http://ec.europa.eu/growth/sectors/medical-devices/index_en.htm. Accessed November 5, 2015.

23. U.S. Food and Drug Administration (FDA). Code of Federal Regulations. 21 CFR Part 11. Electronic records; electronic signatures. Available at: http://www.ecfr.gov/cgi-bin/text-idx?SID=25921bbc80c5b42f23b2a159af340341&mc=true&node=pt21.1.11&rgn=div5. Accessed July 28, 2016.

24. U.S. Food and Drug Administration (FDA). Guidance for Industry: Computerized Systems Used in Clinical Investigations. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiPtdvasJbOAhXCpR4KHcOvCswQFggcMAA&url=http%3A%2F%2Fwww.fda.gov%2FOHRMS%2FDOCKETS%2F98fr%2F04d-0440-gdl0002.pdf&usg=AFQjCNE_paHLgkuPwsRiP1emx8JtpxjeUw&sig2=eOsJEW2dD5lHwmL9VAEc1g&bvm=bv.128450091,d.dmo&cad=rja. Accessed July 28, 2016.

25. European Parliament. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999. Electronic signatures directive. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24118. accessed July 28, 2016.

26. U.S. Food and Drug Administration (FDA). Medical Devices; Current Good Manufacturing Practice (CGMP) Final Rule; Quality System Regulation. Available at: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/QualitySystemsRegulations/ucm230127.htm. Accessed November 5, 2015.

27. U.S. Department of Health and Human Services. Guidance for Industry. E6 Good Clinical Practice: Consolidated Guidance. International Conference on Harmonisation. April 1996. Available at: http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM073122.pdf. Accessed July 28, 2016.

28. Clinical Data Interchange Standards Consortium. Leveraging the CDISC Standards to Facilitate the use of Electronic Source Data within Clinical Trials. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwj804GCrZbOAhVMVh4KHRJwBTAQFggqMAE&url=http%3A%2F%2Fwww.cdisc.org%2Fsystem%2Ffiles%2Fall%2Freference_material_category%2Fapplication%2Fpdf%2Fesdi.pdf&usg=AFQjCNGKy7VMTBuFTvhyz3zm31QQeUiOMg&sig2=okNOEF3ASksNephhQ9kTaw&bvm=bv.128617741,bs.2,d.dmo&cad=rja. Accessed July 28, 2016.

29. U.S. Food and Drug Administration (FDA). Center for Drug Evaluation and Research (CDER), Center for Biologics Evaluation and Research (CBER), and Center for Devices and Radiological Health (CDRH). Guidance for Industry: Electronic Source Data in Clinical Investigations. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB0QFjAAahUKEwign-b4jvrIAhWIVyYKHTxgC6o&url=http%3A%2F%2Fwww.fda.gov%2Fdownloads%2Fdrugs%2Fguidancecomplianceregulatoryinformation%2Fguidances%2Fucm328691.pdf&usg=AFQjCNHfVqVo82GHIQPOe_-hSfpGjfmQrg&sig2=bWAfItcKXGdNqxD4JklHpg&bvm=bv.106923889,d.eWE. Accessed November 5, 2015.

30. European Medicines Agency (EMA). Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB0QFjAAahUKEwiq697Gj_rIAhXIMSYKHQxLBVw&url=http%3A%2F%2Fwww.ema.europa.eu%2Fdocs%2Fen_GB%2Fdocument_library%2FRegulatory_and_procedural_guideline%2F2010%2F08%2FWC500095754.pdf&usg=AFQjCNG55BezxmhjmYqYPeCfv80y1GcbtA&sig2=d-ZoEUSBBiONSLpW3ckFHQ&bvm=bv.106923889,d.eWE&cad=rja. Accessed November 5, 2015.

31. U.S. Food and Drug Administration (FDA). Office of Scientific Investigations website. Available at: http://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDER/ucm090085.htm.

32. Google. Mobile-friendly test. Available at: https://www.google.com/webmasters/tools/mobile-friendly/. Accessed November 5, 2015.

33. Google. Rolling out the mobile-friendly update. Blog. Available at: http://googlewebmastercentral.blogspot.com/2015/04/rolling-out-mobile-friendly-update.html. Accessed November 5, 2015.

34. United States Access Board. Section 508 standards. Available at: http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards. Accessed November 5, 2015.

35. Health Level Seven International (HL7). Mobile health. Available at: http://www.hl7.org/Special/committees/mobile/index.cfm. Accessed November 5, 2015.

36. S&I Framework. BlueButton Plus Initiative. Available at: http://wiki.siframework.org/BlueButton+Plus+Initiative. Accessed July 28, 2016.

37. U.S. Department of Commerce. National Institute of Standards and Technology (NIST). Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Special Publication 800-124 Revision 1. Available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. Accessed November 5, 2015.

Appendix: Mobile Standards to Facilitate Data Collection, Exchange, and Security

Types	Standard	Use	Benefits
Web and usability standards	W3C website design[20]	Website design focusing on technical aspects of graphics, forms, device adaption security and privacy	Easy adoption for devices to be "mobile friendly"[32,33]
	Section 508 standard[34]	Government standards for electronic and information technology including computer hardware and software, websites, phone systems, and copiers	Addresses access to for those with physical, sensory, or cognitive disabilities
	HL7 mobile health standards *(in development)*[35]	Standardize transport of short messages (SMS, text, Twitter) Promote interoperability across apps Standardize data collection	Move away from ad hoc development to define security, costs, privacy, and governance requirements Share data across mobile apps
	FHIR[11]	Mobile, web, exchange protocol for users' health records	Lightweight, compact, ease of use, JSon compatible, Rest Interface, OAuth
	Automate Blue Button, Office of National Coordinator and S&I Framework[36]	Mobile, web apps, small Healthcare orgs, connection to HIE	User's ability to download and share medical records with the push of a button; many companies agree to support standard
	Body Area Network (IEEE 802.15.6)	Body sensors, implants, diagnostics, monitoring (wearables)	FCC allocated band to reduce interference; band with less transmission traffic
	Certificate Interoperability; S&I Framework	Nationwide trust fabric; Certification authorities (CA) to issue interoperable digital certificates	CA standards to minimize costs to maintain, and use digital certificates
	ISO/IEEE 11073	Medical device interoperability	Promote sharing from devices to EHR systems Primarily use, personnel, or end user, health devices, user-reported data
	Integrating the Healthcare Enterprise–Mobile Access to Health Document Profile	Document exchange between mobile devices and EHR or PHR systems.	Promotes interoperability of data in document formats from devices to systems.

Types	Standard	Use	Benefits
Policy standards	NIST mobile standards[37]	Focus on policies and governance in relationship to security and guidance on BYOD	Ensures confidentiality, integrity and availability during transmission and storage using mobile devices
Content standards	Clinical Data Acquisition Standards Harmonization (CDASH)	Creating forms in regulated environments	Standardizing content across studies or trials
	HL7 Domain Analysis Models	Therapeutic Area Data Elements designed for multiple purposes including research and healthcare	Standardizing content at the point of collection and sharing it with various stakeholders including research

Abbreviations: BYOD=bring your own device; CA=certification authority; CDASH= Clinical Data Acquisition Standards Harmonization; EHR=electronic health record; FCC=Federal Communications Commission; HIE=health information exchange; HL7=Health Level 7; NIST= National Institute of Standards and Technology; PHR=personal health record; S&I=standards and interoperability; SMS=short message service; W3C=World Wide Web consortium