Best Practices for Participant Registration in Clinical Trials Using Bring Your Own Device (BYOD) Technology for Data Collection

ePRO CONSORTIUM
CRITICAL PATH INSTITUTE

April 2021

c-path.org/programs/epro

Scope

Mobile technology has completely revolutionized many industries in the past decade. This is also true for clinical trials in which mobile technology, in particular smartphones and tablets, is used to collect patient-reported outcome (PRO) data in the field or at the investigational site. Mobile technology can help the clinical trial sponsor improve participant recruitment, capture better quality data, increase participant compliance, and keep participants engaged in the trial.

Providers of electronic clinical outcome assessment (eCOA) services have historically provisioned devices for clinical trials to make sure participants have access to technology compatible with the needs of the clinical trial. With worldwide increase of smartphone usage and improved access to the internet, eCOA companies started proposing *bring your own device* (BYOD) approaches where BYOD refers to trials in which participants may use their own mobile devices to collect PRO data.

A BYOD approach for PRO data collection offers key advantages, including but not limited to the following:

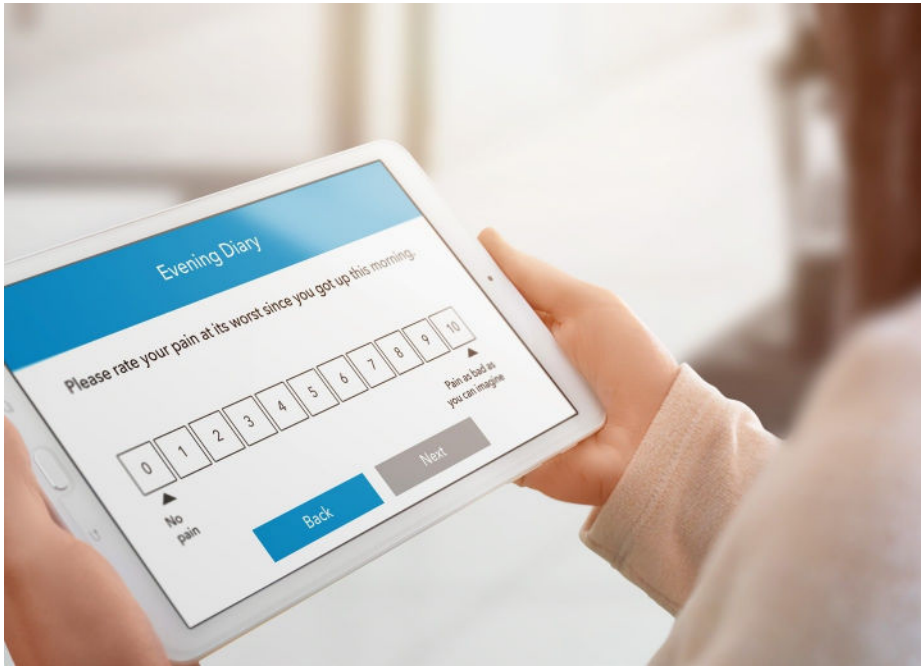
- BYOD can reduce the need for provisioned devices and can simplify logistics, which often involves overcoming customs issues encountered when importing provisioned devices. A small number of provisioned devices may be needed to accommodate participants who do not own a suitable device for the trial.
- BYOD may render patient participation in trials less burdensome. It eliminates the need to carry an extra device for the trial, and because participants are accustomed to using their own device, the need for device-specific training is reduced.
- BYOD may also reduce burden for sites as they don't need to maintain and store as many extra devices.

New technologies usually come with new requirements. Using the participants' own mobile devices might require access to additional personal information such as an email address or mobile telephone number. The scope of this short best practice document is to provide some insights on current participant registration practices to ensure participant confidentiality in clinical trials using BYOD for data collection.

General Considerations

- Prior to the start of the trial, it is important to communicate to participants, ideally in the Informed Consent Form (ICF), how technology will be used to collect PRO assessments. The ICF must explain which data will be collected and why. Accordingly, the ICF must state that personal information will be collected, and participants must acknowledge and indicate (through signature) that they were informed and are willing to provide this personal information. The participants also must be made aware that the technology uses their data plan to download the software application and to send data and receive text messages and notifications. Often, participants are worried about data consumption related to the software application footprint and usage needed for the trial. Clinical trial software applications, however, use very little data. Typical applications occupy, on average, less than 0.5% of the total smartphone capacity, and the monthly data transmission averages less than 1% of the total data plan (e.g., Google Play AZCure App, TrialMax App, mProve App, YPrime App, Clinical Ink Engage App). The reimbursement policy for data plans, if any, should be addressed in the ICF.

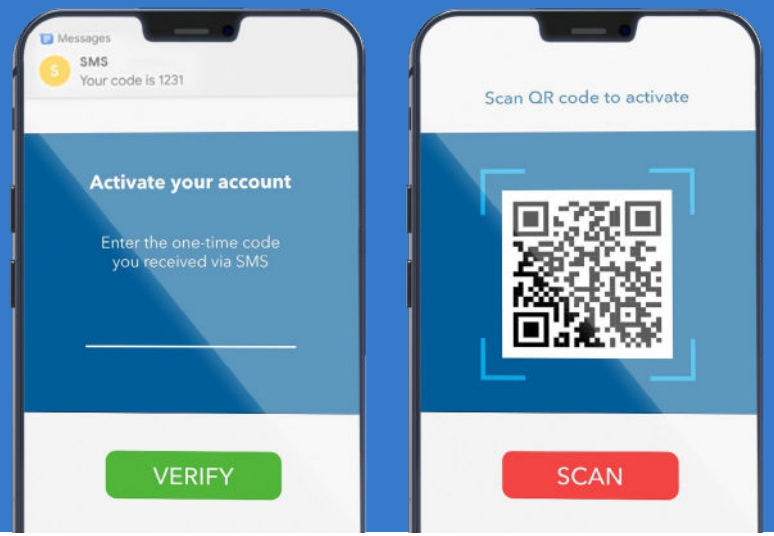
- Data protection information must also be communicated to the participants by explaining that any personal information collected during the trial will be protected in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and the EU General Data Protection Regulation (GDPR). Clinical trial data are considered a 'special' category for which processing is necessary for scientific and research purposes. This special data category negates the participant's right to erasure, or portability; hence, participants must be made aware that they can prevent additional data collection only by leaving a trial, and that the data already collected will not be deleted. This conclusion is shared by data protection law experts: "While research uses of personal data do not create an absolute exception to right of erasure, a data processor can refuse an erasure request following a withdrawal of consent if it can either (1) establish an alternate legal basis, such as legitimate interests, or (2) demonstrate that deletion of the data related to the data subject will seriously impair the research objective." [1]



In terms of access to sensitive information such as personally identifiable information (PII), eCOA providers should access decrypted mobile numbers or email addresses only in cases of support or troubleshooting needs. After such PII has been used, all evidence should be immediately deleted, including deletion from recycle bins from all computers where the decrypted information was used. Any decrypted information shared with sponsors must be completely de-identified. Some systems, leveraging differing approaches to dual factor authentication, have been able to bypass any use of PII related to participant registration and login.

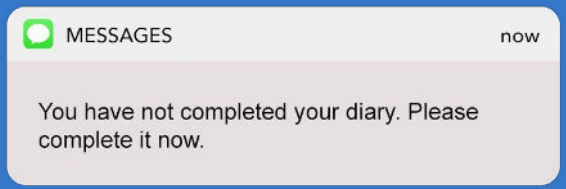
The participant mobile number can be used to send and receive text messages through Short Message Service (SMS). Text messages have been used for decades by billions of people across the globe and have become extremely user friendly [2]. In a trial utilizing BYOD, SMS can serve multiple purposes. Participants can use it to send messages to the investigative site to reschedule a visit, it can be used to direct the participant to the software location in the application store or to send activation codes that will allow participants to initialize the application and to start completing assessments. A web link can be embedded in the SMS message. The participant must select it in order to be automatically directed to the appropriate location to download the clinical trial software application or enter the activation code (Figure 1). Alternatively, the eCOA provider could send a QR code or a scan/bar code with similar functionalities via email to the participant which can be scanned using the camera on their device for access to the application directly within the corresponding application store. These activation codes have often limited time validity to avoid malicious use.

Figure 1: Activation screens



SMS messages are also used to send notifications (Figure 2) or alerts to the participants. Such notifications or alerts can include reminders to attend study visits, perform an action, or to complete assessments. These messages can also be formatted to keep the participant engaged in the trial. Sending a message such as the following one encourages the participant to continue their assessments.

Figure 2: Example of notification sent by SMS



- Participant email addresses can also be collected for similar purposes. Rather than an SMS, an email containing weblinks can be sent to the participants allowing them to download the initial application or to connect to a web portal. Like SMS, emails can be used to send notifications and alerts to the participants with the purpose of keeping them engaged. However, a mechanism allowing the participant to opt out of such notifications should be made available to protect the participant's privacy. Ideally, the participant should be able to choose a preferred method of communication. This, however, could vary based on the technology offered by the eCOA provider.

- Once the clinical trial software application is downloaded and activated on the participant's mobile device, the participant is provided access to various services based on clinical trial needs. At a minimum, the participant will be provided access to self-reported data collection tools (e.g., PRO measures or event diaries) that require completion based on the protocol requirements. Also, notifications and alerts remind the participant to complete the assessments at a scheduled time. Data the participants record will be stored locally on the mobile device in an encrypted format until the data are transmitted to the eCOA provider's server. Data should be transmitted as soon as possible, meaning as soon as a communication channel (e.g., WiFi, cellular) has been established, in order to limit the loss of data in case of device failure or loss. Once transmitted and backed up on the server, data can be automatically removed from the participant's device in order to free storage space unless those data are needed for calculating the next visit, history of events, or for triggering other assessments or alarms.

- For participant engagement purposes, a variety of additional services can be made available to the participant such as a progress bar, easy access to site details (such as location and phone numbers), user guides, videos, reimbursement information, gamification, and even Uber or Travel Concierge services for transportation to/from site. For these services, PII, such as the participant's phone number, could be used but would not be made accessible to unauthorized personnel.

- At the end of the trial, once all data have been transmitted, the participant should delete the application from their mobile device. Sites will archive the participant's profile in their database. Any remaining PII must be anonymized.

Conclusion

BYOD technology is slowly but surely becoming more prevalent in the clinical trial context and is often used for participant recruitment, participant retention, and for collecting clinical outcome assessment data. Alerts and notifications can be easily sent to remind the participant to complete an assessment, perform an action, or attend a site visit. These types of alerts and notifications help participants feel more connected and engaged [3]. Additional PII, such as mobile numbers and email addresses, are collected for this purpose; however, the information should be visible only to the investigator and authorized personnel and never communicated to the trial sponsor. Processes must be in place to help ensure HIPAA and GDPR compliance and thus, protection of participant privacy.

References

1. Hintze M. Science and Privacy: Data Protection Laws and Their Impact on Research. 2019. *Washington Journal of Law, Technology & Arts*. 4:18.

2. International Telecommunications Union. The World in 2010: ICT Facts and Figures. Available at:*http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf*

3. Perri-Moore S, Kapsandoy S, Doyon K, Hill B, Archer M, Shane-McWhorter L, et al. Automated alerts and reminders targeting patients: A review of the literature. 2016. *Patient Education and Counseling*. 99:953-959.