Emerging Issues in Using Mobile Apps for Clinical Research

By Nathan Prystowsky and Jonathan Walland

Since the advent of smart phones, lawmakers and regulators have been slow to react to the exponential development of mobile health apps. Health lawyers faced with advising clients on the first generation of mobile health apps faced the daunting task of trying to situate novel technologies onto laws that were promulgated in a pre-digital age: Could a given app be deemed a medical device subject to FDA regulation? When are use and disclosure of medical information in an app subject to the provisions of HIPAA? Are direct-to-consumer health apps created by non-medical entities subject to any kind of regulation?

Recent settlements, FDA guidance, and safe harbors for limited functionality health apps have provided some emerging frameworks and regulatory assurances. However, a key area of regulatory uncertainty remains in the use of mobile health apps for clinical research. Depending on the research aims and the nature of the parties conducting and sponsoring a given research study, it may be subject to an overlapping web of laws, regulations, and standards including the Federal Policy for the Protection of Human Subjects (also known as the "Common Rule"), FDA drug or device testing regulations, and G.C.P. (Good Clinical Practice). A recurring theme they all share, is the paramount importance of data reliability and accuracy.

Historically, clinical research data has been generated and collected by trained healthcare workers using standard collection methods and verifiable source documents. But smart phone-enabled mobile health apps offer the tantalizing prospect of real-world, continuous, and real-time interaction with research subjects. A number of use cases exist for mobile health apps in a research context:

- A mobile app might be used to collect self-reported data from research subjects;
- A mobile app might be used as a health intervention;
- A mobile app might be used to collect and measure quantitative biometric values from a research subject using a smart phone's built-in functionality or peripherals including wearables.

We hypothesize that both regulators and study sponsors will increasingly be interested in using mobile apps for the third purpose, in order to provide more reliable real-time data that is potentially superior to the "snapshot" approach provided by weekly or monthly research subject visits to an investigator's laboratory or clinic. Yet two intertwined challenges remain to the widespread implementation of mobile apps in clinical research: (i) the need to validate the technology behind mobile health apps, and (ii) the need to develop regulatory frameworks that support the use of mobile health app technology in research.

This article will begin with an overview of the challenges raised by using mobile health apps and devices in a research context. We will summarize the regulatory landscape for mobile health apps and offer suggestions for lawyers advising clients who want to conduct research involving mobile apps in the life sciences sector.

FDA Regulation of Mobile Apps

The FDA's 2015 Guidance on Mobile Medical Applications, defined mobile application or "mobile app" as "a software application that can be executed (run) on a mobile platform (i.e., a handheld commercial off-the-shelf computing platform, with or without wireless connectivity), or a web-based software application that is tailored to a mobile platform but is executed on a server."[1] An enhanced category of mobile medical app was designated for mobile apps that also satisfied the Food Drug and Cosmetic Act's criteria for a medical device *and* were intended "to be used as an accessory to a regulated medical device; or to transform a mobile platform into a regulated medical device."[2] Initially, the underlying criteria for whether a mobile app should be deemed a medical device drew on the familiar FDA analysis of whether it was meant for "the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function" of the human body. These criteria were further modified by the medical device definition in the 21st Century Cures Act and subsequent guidance, which moved some examples of mobile apps for which FDA intends to exercise enforcement discretion to the class of mobile apps that FDA categorically deems not medical devices.[3]

FDA guidance has identified three broad categories of mobile app technology that would be deemed "regulated medical devices," subject to one of the existing medical device approval pathways (e.g., premarket review, 510(k) exemption etc.): (i) mobile apps that connect to a medical device for purposes of active patient monitoring,

Jonathan Walland, Esq. is Senior Corporate Counsel at Pfizer Inc. and is admitted as an attorney in New York. Previously he was Associate General Counsel at the Memorial Sloan-Kettering Cancer Center. **Nathan G. Prystowsky, Esq.** is the Secretary of the NYSBA Health Law Section and Co-Chair of the E-Health and Information Systems Committee. Mr. Prystowsky works at Janet H. Prystowsky, M.D., P.C. where in addition to other duties he manages the Information Technology Governance of the Practice.

or analyzing medical device data; (ii) mobile apps that transform a mobile platform into a medical device by using attachments, display screens, sensors or by including functionalities similar to those of currently regulated medical devices; and (iii) mobile apps that function as regulated software by performing patient-specific analysis, diagnosis, or treatment recommendations.

The FDA guidance provides instructive examples of technology across disparate medical disciplines that would likely fit the foregoing criteria: (i) apps that provide the ability to control inflation and deflation of a blood pressure cuff through a mobile platform; (ii) mobile apps that control the delivery of insulin on an insulin pump by transmitting control signals to the pumps from the mobile platform; (iii) mobile apps that use peripheral attachments to perform medical device functions, such as attachment of a blood glucose strip reader to a mobile platform to function as a glucose meter; (iv) attachment of electrocardiograph (ECG) electrodes to a mobile platform to measure, store, and display ECG signals; (v) a mobile app that uses the built-in accelerometer on a mobile platform to collect motion information for monitoring sleep apnea; (vi) a mobile app that uses sensors (internal or external) on a mobile platform for creating an electronic stethoscope function, thus transforming the mobile platform into an electronic stethoscope; (vii) patient monitoring mobile apps that monitor a patient for heart rate variability from a signal produced by an electrocardiograph, vectorcardiograph, blood pressure monitor and would be classified as cardiac monitoring software; and (viii) treatment planning software apps that use patient-specific parameters and calculate dosage or create a dosage plan for radiation therapy.

On the other end of the spectrum, are "low risk" technologies and functionalities which FDA has repeatedly identified in its guidance for enforcement discretion, or more recently under the 21st Century Cures Act, as irrefutably "not regulated devices."[4] These include many consumer and health care provider (HCP) health apps intended to: (i) help coach patients to make diet, exercise, and lifestyle improvements, (ii) help patients track and organize their health information; (iii) serve as EMR portals that enable patient access to medical records and related instructional health articles to manage symptoms; (iv) serve as telemedicine portals that enable patients to communicate with HCPs via a device's sound and video functionality; and (v) function as HCP clinical tools that perform very basic calculations such as Body Mass Index.

Use of Mobile Apps and Wearables in Traditional IRB-Approved Research

Initial deployment of mobile apps in clinical research was often focused on collection of patient self-reported data, including electronic pill diaries to monitor investigational drug adherence, symptom diaries, adverse event recording, and patient reported outcomes. One of the earliest sources of recommendations was the FDA's December 2009 guidance document, "Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims."[5] This guidance defined patient reported outcomes (PROs) as "any report of the status of a patient's health condition that comes directly from the patient, without interpretation of the patient's response by a clinician or anyone else."[6] FDA included suggestions on the type of information suitable for PRO data, generally measurement of patient symptoms, disease severity, and other concepts best known by the patient or best measured from the patient perspective.[7] Of particular interest for this article, was the guidance included in Section IV. Clinical Trial Design, Subsection F. Specific Concerns When Using Electronic PRO Instruments.

In a research context, mobile health app data, including PRO data, would be considered a source document. Accordingly, Subsection F raised several notable concerns about the need for data reliability, including compliance with FDA's electronic data integrity standards set forth in 21 C.F.R. § 11, and the need for investigators to ensure accurate record keeping, maintenance, and access.[8] Another key takeaway, was FDA's emphasis on the proper allocation of responsibilities between sponsors and investigators. Because investigators are expected to control source documents, FDA identified potential pitfalls when research sponsors control electronic PRO tools. FDA recommended that to satisfy the regulations, sponsors should not have exclusive control over electronic tools that will be relied upon as source documents, and that adequate audit trails exist to ensure data are not modified.[9]

For clinical researchers interested in measuring bodily function by collecting biometric device data from a mobile app or wearable, the regulatory analysis should include consideration of validation and testing to confirm the accuracy and reliability of data generated. This is especially true if the mobile app or wearable functionality crosses the line into the realm of "regulated medical device." One could imagine a drug study conducted under an Investigational New Drug (IND) application that uses an unapproved medical device requiring its own regulatory pathway for an Investigational Device Exemption (IDE). Validation of such mobile app or wearable for clinical research uses might require pilot testing or head-to-head comparisons with traditional data generated from clinic visits, laboratory analysis, and physician-validated assessment tools. Research sponsors will invariably face the question of how much validation is needed before a mobile app or wearable can be deemed sufficiently robust to be deployed in a research study to gather submission-quality data.

Although concerns about data privacy and confidentiality have practically monopolized recent technology discussions, we argue that traditional issues of quality and data integrity should be the starting point when developing mobile apps and wearables for clinical re-

search. Data integrity is defined as the extent to which data are complete, consistent, accurate, trustworthy and reliable.[10] Clinical research auditors have historically used the acronym ALCOA as a pneumonic descriptor of the relationship between source documents and the data captured onto case report forms or electronic data capture systems—data should be attributable, legible, contemporaneous, original, and accurate.[11] For FDA-regulated clinical research that will be used as part of a submission for a new drug or device application, the standards set forth in 21 C.F.R. § 11 establish minimum criteria for data integrity and reliability. These regulations distinguish between "open" versus "closed" systems. An open system is one in which control of the system is not in the hands of the individual responsible for generating the content of the electronic record. Relying on data from mobile apps and wearables can pose challenges for authenticating the identity of users and the veracity of information collected. Outside of the controlled clinic environment, a research subject might allow another household member to use a mobile device or wearable. To what extent must research sponsors and investigators authenticate the identity of the mobile app users? Should such authentication be a one-time event when logging in or setting up the device? Should there be periodic checks? How might the reliability of data gathered from a mobile app or wearable differ from data collected by an investigator or research coordinator in a clinic setting?

The Food Drug and Cosmetic Act as well as regulations under 21 C.F.R. §§ 50 and 56 protect human subjects participating in research for clinical trials. Generally, consumer mobile health apps are not marketed as clinical support medical devices that fall under 21 U.S.C. § 321 (h). When a mobile health application counts as "software as a medical device" (SaMD under 21 U.S.C. § 321(h)), it then requires an Investigational Device Exemption (IDE) under 21 C.F.R. § 812. This in turn further requires an analysis of device in the trial for significant risk (SR), non-significant risk (NSR), or exempt status.

While consideration of SaMD devices goes beyond the scope of this article, it is worth noting that using mobile health applications that fall outside of the SaMD regulatory framework can lead to clinical validation issues. Devices outside of the SaMD framework presumably have not gone through the FDA recommended principles of software validation. The FDA has required software validation as part of its design control provisions under 21 C.F.R. § 820.30(g) in addition to other validation requirements under 21 C.F.R. § 11.10(a).

Industry guidance has been developing along with technology to account for the appropriate compliance considerations for software generally in the clinical research setting. New guidance for collecting data from electronic health record (EHR) systems that are interoperable with Electronic Data Capture Systems (EDC) for clinical trials touches on many of the of the same interoperability points of consideration for using a mobile health application.

The Office for Human Research Protection in the Department of Health and Human Services (OHRP) recommends that institutions have policies in place that designate an individual or entity authorized to determine whether research involving coded private information constitutes human subject research. In the event the authorized individual or entity determines the investigator will know or may be able to readily ascertain the identity of the individuals to whom the obtained private information pertains, it would be considered human subject research.

A human subject is defined by Federal Regulations as "a living individual about whom an investigator conducting research obtains (1) data through intervention or interaction with the individual, or (2) identifiable private information." (45 C.F.R. § 46.102(e)(1)). Identifiable private information "includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation is taking place" (such as a public restroom) "and information which has been provided for specific purposes by an individual and which the individual can reasonably expect will not be made public (for example, a health care record)." (45 C.F.R. § 46.102(e)(4)).

IRB review of a proposed research study is required unless the research project is determined to be exempt under HHS regulations at 45 C.F.R. 46.104. Otherwise, informed consent of the subjects would be required unless the IRB approved a waiver of informed consent under 45 C.F.R. §§ 46.116(c) or (d). In the health care setting informed consent can be particularly problematic because HIPAA restricts the ability to obtain a compound individual privacy authorization, except in limited circumstance. For example it may be possible incorporate a HIPAA Privacy authorization into a research consent in accordance with 45 C.F.R. § 164.508(b)(3) and (4).

As with IRB studies outside of FDA approved clinical trials, there are issues with respect to obtaining the consent of subjects. When informed consent is required, the consent must include a statement describing the extent, if any, to which confidentiality of records identifying the subject will be maintained according to 21 C.F.R. § 50.25(a)(5). Since the FDA may inspect and copy records relating to clinical investigations under 21 U.S.C. § 374 (a)(1) and 21 C.F.R. §§ 312.58(a), 312.68, and 812.145(b) the consent process should describe the possibility that FDA inspectors and FDA submission reviewers may need to review source material and electronic logs for mobile app data, which in some cases may include communication between the research subject and HCPs. While some EHR systems include audit mode capabilities that permit regulatory inspection of medical records in a secure environment with direct patient identifiers removed, this functionality might not exist in novel health and medical apps.

It is also worth noting that mobile health applications are not always capable of transmitting data in a format that will be interoperable with the intended data depository. The software being used to house, access, and analyze the data in the research data repository often has a different format that creates an obstacle hindering the transmission and storage of data from a mobile health application. This has implications for data integrity in long-term storage situations where research may extend beyond the lifecycle of the software. Consequently, data management centers also need to be aware of data retention requirements.

Under 21 C.F.R. §§ 312.62, 511.1(b)(7)(ii) and 812.140, the clinical investigator must retain records required to be maintained under §§ 312, 511.1(b), and 812, for a period of time specified in these regulations. The retention period should not be ignored. "White listing" software upgrades throughout the software lifecycle (i.e., the process of validating interoperability of new versions with other interfaced software applications) is necessary to preserve data integrity while also meeting the need to update software that addresses current vulnerability threats in the cyber security framework of the institution housing the research data repository. These issues become especially relevant and challenging if expired "legacy systems" that preserve data become inaccessible. For example, the early generation iPhones have been sun-setted by Apple, making them nearly unusable with current operating systems and network environments.

Finally, in November of 2018, the FDA launched the MyStudies app website, which includes open source code to enable researchers and app developers to link real world data and electronic health records in order to support high-quality collection and use in regulatory submissions.[12] These tools are intended to comply with the requirements of 21 C.F.R. § 11 and enable efficiencies in the drug development and safety monitoring process.[13] In the long term, the ability to harness real world evidence through so-called "pragmatic clinical trials" might improve patient experience and accelerate the drug development process. On the other hand, this may lead to a diminished role for experienced clinical investigators and researchers, as the clinical research and standard care world will increasingly converge. Questions remain on how IRBs, sponsors, and investigators will ensure adequate protections for human research subjects if everyone's smart phone becomes a medical data collection tool. These concerns have already started to surface in the field of consumer health apps.

Clash of the Civilizations: Disruptive Technology and Consumer Health Apps Meets Research Regulators

Before the growing prevalence of mobile health applications, the Institute of Medicine charged a Committee on Health Research and the Privacy of Health Information to assess the HIPAA Privacy Rule and make recommendations on facilitating health research while maintaining protections for individual privacy. In its 2009 report, the committee noted "public opinion polls suggest that a significant portion of the American public would like to control all access to their medical records for research via an individual consent mechanism."[14] Mobile health apps have broad applications in these various types of regulated research because of their ability to generate large quantities of scalable data.

Consumer health apps that collect health data are already being used to support human subject research covering a broad spectrum from recording vitals during FDA-approved clinical trials and minimal risk IRB-approved behavioral research. For this reason, researchers need to take into account important considerations with respect to the types of data being generated in the research setting and whether that data is protected data under a regulatory scheme limiting its use in a research setting.

The modern era of technology innovation has been marked by a distinct obliviousness to legal and regulatory requirements in the interest of speeding products and services to market. In diverse areas such as online gambling, taxi car service, and employee benefits, enthusiastic tech entrepreneurs have launched start-up companies despite in many cases being unfamiliar and non-compliant with existing legal frameworks, or in other cases, choosing to deliberately ignore them.

Health apps are no exception to this trend. Many early health apps were developed by non-health care entities, unfamiliar with potential privacy concerns or perhaps emboldened by their status as non-HIPAA covered entities and their direct-to-consumer business model. In many cases, user health data was collected and analyzed for commercial data aggregation/monetization purposes, or as part of research studies intended to validate a mobile health app's purported benefits. For example, the 2014 launch of Apple's HealthKit created a common framework for developers to share patient-generated health data (PGHD) among apps, services, and providers, which at one point had over 1,500 apps developed that could make use of a variety of PGHD including: data collected, captured step counts, body measurements, vital signs, exercise patterns, nutrition, reproductive health, and sleep.[15] These adjuvant research uses of both fitness and health-related mobile apps, initially caught lawmakers and stakeholders off guard, and triggered a slow but growing wave of regulation. Among the key concerns: data privacy, data governance, and data permissioning.

Consequently, consumers have a growing concern over what happens to their data, and data collected by consumer wearables often does not have any relationship to a covered entity and as such does not get protected by HIPAA. With the growth of health information data collected outside of the protected regulatory framework

of HIPAA, or the IRB and FDA approval processes for research, other agencies have taken action to use broad consumer protection laws to create privacy protections for mobile health applications.

The Federal Trade Commission (FTC) has designed a consumer protection framework that requires certain disclosures in the End User License Agreement (EULA). Section 5 of the FTC Act authorizes the Commission to challenge "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a). In April 2016, the FTC launched a Mobile Health App web portal intended to help guide developers towards regulatory compliance, by highlighting some of the applicable laws in the field.[16] The site includes a HIPAA privacy decision tree tool, to help determine which regulations might apply to mobile health app developers.

Of particular interest for New York health lawyers, the Attorney General's Office (OAG) has relied on the same consumer protection framework to aggressively prosecute direct-to-consumer health app companies for perceived shortcomings in device efficacy, privacy disclosures, and research practices.[17] In a trilogy of settlements announced in 2017, three mobile health app manufactures paid fines and agreed to cease making unsupported functionality claims and bolster privacy risk disclosures to consumers. The settlements involved the My Baby's Beat–Baby Heart Monitor App, the Heart Rate Monitor, Heartbeat & Pulse Tracker, and the Cardiio-Heart [*sic*] Rate Monitor.[18] The OAG faulted the companies for launching the products without adequate device validation and for gathering and sharing user data, including in some cases health information, without informing users that such data might not be protected by the HIPAA Privacy Rule.[19] It is unclear to the authors if a court would necessarily agree and impose an affirmative duty on a non-HIPAA covered entity to inform users that they are not subject to the HIPAA Privacy Rule, Security Rule, and Breach Notification Rule, but there are several noteworthy clinical research concerns raised by the OAG in these cases.

From a consumer protection perspective OAG was displeased that all three app developers had launched their products without sufficient testing. This was reflected in the settlement language emphasizing OAG's belief on validation testing: "The testing must be performed by researchers qualified by training and experience to conduct such testing."[20] It seems clear that mere reliance on software developers and product engineers may not be enough. The regulators seem to be demanding that mobile health apps be validated by researchers with clinical research training and experience, especially mobile health apps that might satisfy the earlier referenced FDA criteria for regulated medical devices—i.e., those that measure or monitor critical patient health conditions or seek to replace existing regulated medical devices. Requiring mobile health app developers to conduct validation studies may hamper innovation by adding to production costs and product development timelines.

From a privacy protection perspective, OAG faulted all three app developers for inadequate disclosures on how they might aggregate, analyze, and disclose user information to third parties. Although the settlements do not make clear the extent to which the companies might have intended to aggregate and monetize user health information for subsequent research, OAG asserted that collecting health data without clear warnings and user consent would be seen as violations under NY General Business Law §§ 349 and 350, and under NY Executive Law § 63(12) deceptive business practices. This is especially noteworthy because many consumer health apps have built their business model with an eye to non–IRB-approved research consisting of user data aggregation and data mining analytics.

The Next Frontier: Mobile Health Apps Data Aggregation and Data Mining

The Office of the National Coordinator for Health Information Technology (ONC) has recognized that PGHD from consumer devices has the ability to enhance future health care and research.[21]

As an example, the ONC has recognized that research-oriented platforms, such as Apple ResearchKit, offers new recruitment methods that may speed up research studies by increasing the rate of enrolment and making it easier to build a dataset sufficient for analysis.[22] The exploration of using PGHD from consumer devices has led to initiatives, such as the Precision Medicine Initiative, which are being supported by the National Institute of Health (NIH) and ONC by a Sync for Science pilot program, which is "developing and testing the technology to enable patients to share data from their clinicians' EHRs with researchers."[23]

Data generated by a mobile health application generally is classified in two ways. In its broadest sense, individual health information generated, collected, and then aggregated by a consumer health application is classified as Individually Identifiable Health Information (IIHI). More narrowly, IIHI that is created, received, maintained, or transmitted by a HIPAA covered entity (e.g., health plan, health care provider, or business associate) would be considered Protected Health Information under HIPAA.[24] Conversely, health information shared by a consumer or between two consumers, independent of a covered entity or business associate is not PHI under HIPAA.

However, as noted above, even if IIHI does not become PHI under HIPAA it does not mean that the data can be freely used. In the research setting there are three broad sets of regulations that protect individuals who volunteer their data to entities that seek to collect and make use of that data for study. The Food Drug and Cosmetic Act as well as regulations under 21 C.F.R. §§ 50 and

56 protect human subjects participating in research for clinical trials. Human subject research for generalizable knowledge requires compliance with 45 C.F.R. § 46 (the "Common Rule") for the protection of human subjects. Even if a given mobile health app research project would be exempt from FDA regulation or the Common Rule, in New York it might be subject to the New York State clinical research laws under § 24-A of the Public Health Law.[25] Although § 24-A contains exceptions for epidemiological research and is focused on interventional research, it does notably include psychological interventions where there is no underlying therapeutic intent.

We believe that regulatory pressure, media scrutiny, and growing public awareness might push mobile health app developers to limit mobile health app data aggregation and data mining activities, or pursue a formal IRB review and approval before embarking on big data analyses of health data generated by consumer health apps.

Technical Regulatory Considerations for Aggregating Mobile Health Data and Developing Mobile Health Apps

Research sponsors and companies thinking of developing mobile health apps might consider engaging a vendor to develop the software or technology that will be used for research purposes. Such vendors might be unfamiliar with privacy requirements and FDA data validation requirements. Accordingly, contracts with such vendors should carefully address questions of intellectual property ownership, allocation of risk for liability, and indemnification. In addition, attention should be paid to permitted uses of data, privacy considerations, breach notification, data integrity, and data transfer.

In the electronic environment most data will exist in one or more Structured Query Language (SQL) databases, which are known by the technical term "instances," that are run by a larger software program functioning for a particular industry purpose. One industry purpose would be an ONC-certified EHR system. Whether the information collected from a mobile health application goes directly into an EHR, an academic research database, or an FDA-regulated EDC System often changes the analysis of how the data gets protected under the different regulations governing human subject research.

Once the data migration path from the mobile health application to the larger database is determined, further analysis is needed to ascertain how to create a data repository for mining purposes. To begin, a person charged with identifying the applicable regulatory framework should ask whether the mobile health app creates, receives, maintains, or transmits identifiable information. If "yes," the legal analysis might then turn to consideration of the connection between the mobile health app and any applicable covered entity under HIPAA.[26] If the consumer downloads a mobile health application and directs it to transmit health data to an EHR that interoperability arrangement alone does not create a business associate relationship with the developer.[27] On the other hand, if the provider has a contract with the developer to perform a covered function (e.g., for remote patient monitoring), such developer may very well be creating and maintaining that data on behalf of a covered entity.[28]

If a proposed study makes use of a mobile health app with a relationship to a covered entity that cannot be avoided, it is worth considering whether the data can be de-identified using an approved method, as described below. The advantage of de-identification is that the HIPAA Privacy Rule permits disclosure of de-identified information, since it would no longer be considered PHI. However, without de-identification the recipient of data may have to enter into a data use agreement spelling out certain safeguards required under the Privacy Rule.

The other advantage of using de-identified information is that whether a given study is human research depends upon the definition of human subject under 45 C.F.R. § 46.102(e)(4). Obtaining identifiable private information becomes individually identifiable according to the OHRP when it can be linked to specific individuals by the investigator(s) either directly or indirectly through coding systems.[29]

There are two ways of de-identifying data under HIPAA: (1) the expert determination method under § 164.514 (b)(1) or (2) the safe harbor method under § 164.514 (b)(2). The expert method requires a person with "appropriate knowledge of an experience with generally accepted statistical and scientific principles" to evaluate the data set. Alternatively, the safe harbor method requires the removal of eighteen (18) specific identifiers.

If the research can be performed with de-identified data, then best practices would be to go through one of the de-identifying processes to assemble the data repository for research. However, the Institute of Medicine has noted that many researchers find using de-identified data sets problematic because the lack of essential identifiers causes a form of self-selection that can bias results and moreover limits the ability to use available metrics that genuinely impact the outcome of a given study.[30] Another emerging concern is the risk of re-identification, as computing power increasingly allows for the re-identification of individual subjects using minimal amounts of information from de-identified datasets with available information from social media networks, public records, and other sources.

Conclusion

Mobile health app technology continues to evolve and will increasingly play a role in clinical research, as a data gathering tool where an investigational product is being tested, where the health app itself is being validated, and for collection of real world evidence. Companies and researchers interested in using mobile health apps

and wearables for research still face uncertainty and conflict between a myriad of state and federal rules designed for a pre-digital era.

Familiarity with relevant laws and guidance can help lawyers skillfully navigate and advise clients on this rapidly evolving space, with an eye to generating reliable, high-quality research data and ensuring human subject protection.

Endnotes

1. Mobile Medical Applications, Guidance for Industry (2015).
2. Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 321(h) (2018).
3. Changes to Existing Medical Software Policies Resulting from Section 3060 of the 21st Century Cures Act, Draft Guidance for Industry (2017).
4. *Id*.
5. "Patient-Reported Outcome Measures: Use in Medical Product Development to Support Labeling Claims, Guidance for Industry (2009).
6. *Id*.
7. *Id*.
8. *Id*.
9. *Id*.
10. Michael Rutherford, MS, *CH E6(R2) and Data Integrity: Four Key Principles Clinical Researcher*, Clinical Researcher—April 2018, April 17, 2018, (Vol.32, No. 4).
11. *Id.*
12. *See* FDA's MyStudies Application (App), https://www.fda.gov/Drugs/ScienceResearch/ucm624785.htm (last visited Dec. 12, 2018).
13. *Id*.
14. *See* Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule; Institute of Medicine, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research (Sharyl J. Nass, Laura A. Levit, and Lawrence O. Gostin, ed., 2009), at 35.
15. Nicholas Genes et al., *From smartphone to EHR: a case report on integrating patient-generated health data*, npj Digital Medicine (2018) https://doi.org/10.1038/s41746-018-0030-8.
16. *See* Mobile Health Apps Interactive Tool, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool (last visited Dec. 10, 2018).
17. NY Office of the Attorney General, *A.G. Schneiderman Announces Settlements With Three Mobile Health Application Developers For Misleading Marketing And Privacy Practices*, NY Office of the Attorney General Press Release, March 23, 2017, https://ag.ny.gov/press-release/ag-schneiderman-announces-settlements-three-mobile-health-application-developers.
18. *Id*.
19. *Id*.
20. *Id*.
21. *See* The Office of the National Coordinator for Health Information Technology, *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research Through 2024*, January 2018, https://www.healthit.gov/sites/default/files/onc_pghd_practical_guide.pdf.
22. *Id.* at 20.
23. *Id*.
24. *See* Office for Civil Rights, *Health App Developers: Questions about HIPAA?*, https://hipaaqsportal.hhs.gov/ (follow "Answered Qs" hyperlink and scroll down to Clarify when online consumer information is PHI).
25. NY Pub Health Law § 2441 (2012).
26. *See* Health App Use Scenarios & HIPAA, https://hipaaqsportal.hhs.gov/ (follow "Health App Use Scenarios & HIPAA" hyperlink, February 2016.
27. *Id.*
28. *Id.*
29. *See* Coded Private Information or Specimens Use in Research, Guidance for Industry (2008).
30. *See* Nass and Gostin, *supra* note 14, at 232.