AMERICAN HEALTH LAW ASSOCIATION

HEALTH LAW WEEKLY

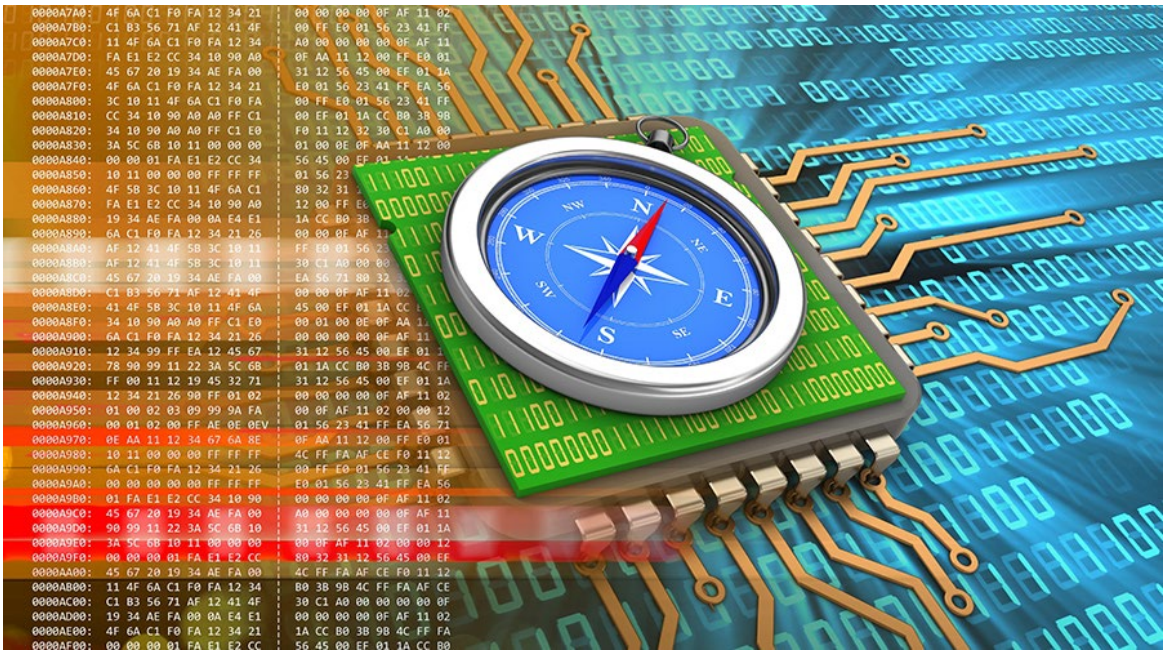
June 14, 2024

NIH Develops Key Considerations and Sample Language for Informed Consent for Research Using Digital Health Technologies

David Peloquin, Ropes & Gray LLP

Leslie Thornton, Ropes & Gray LLP

Carolyn Lye, Ropes & Gray LLP



On May 20, 2024, the National Institutes of Health Office of Science Policy (NIH OSP) released a resource document entitled "Informed Consent for Research Using Digital Health Technologies: Points to Consider & Sample Language" (Resource), which provides key considerations and sample language for research teams and Institutional Review Boards (IRBs) to use when developing and conducting studies that utilize digital health technologies, such as wearable devices, sensor technologies and mobile software applications.[1] The Resource aims to assist researchers in developing materials that promote potential study participants' understanding of the unique data privacy and security risks created by digital health technologies. NIH OSP finalized the Resource after

considering comments received in response to a Request for Information issued on October 11, 2023.[2]

The research community continues to adopt digital health technologies—whether to access new data types or a larger volume of data, to increase participant diversity and/or study population scale, to reduce research-related costs or to adapt study procedures out of necessity (e.g., COVID-19 pandemic). As digital health technologies increasingly are incorporated into scientific research, research institutions, individual researchers and funders should understand their responsibility to communicate effectively to potential study participants the risks, benefits and costs associated with participating in a research study that involves digital health technologies, to ensure that potential participants are, in fact, providing *informed* consent. While use of the Resource is voluntary and is not intended to replace IRB oversight or existing informed consent requirements, it is a helpful starting point for research institutions and researchers to develop and/or tailor informed consent language for use in research studies with digital health components such as tablets, watches or phones.[3]

The Resource provides key considerations and sample language for several components of a standard informed consent document, including components related to procedures, data sharing and ownership and potential risks and benefits. While fairly comprehensive, these key considerations and sample language do not address certain other obligations that investigators may need to consider as part of the informed consent process (e.g., regulatory requirements under the Common Rule or the U.S. Food and Drug Administration's (FDA) regulations governing the protection of human subjects),[4] the incorporation of an authorization to use and disclose protected health information (PHI) pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in connection with the research, the future use of data collected from digital health technologies, as well as broader requirements under NIH's Data Management and Sharing Policy.[5] Nor do they address other recent legal developments in this area, such as subregulatory guidance and enforcement actions related to online tracking technologies or data sharing requirements under the Information Blocking Rule.

Below, we summarize certain key considerations outlined in the Resource, discuss implications for key stakeholders, including research institutions, researchers and funders, and discuss other evolving laws and regulations that may be implicated by the use of digital health technologies in studies.

Summary of Key Considerations for Informed Consent Language for Research Using Digital Health Technologies

The Resource focuses on seven components of informed consent language:

- **Component 1: Introduction.** The purpose of the introduction component is to describe the digital health technologies used in the study, how the technology will be used to help the research study team achieve study goal(s), whether the technology has been cleared by FDA for its intended use (if so regulated) and whether the efficacy of the technology itself is being studied. This component also will describe whether use of the digital health technology is mandatory for participation, what the study participant must do to use the technology (e.g., whether data will be accessed via Wi-Fi or Bluetooth, whether participants' cellular data plan may be affected), whether the digital health technology is proprietary to the research study team or a third-party commercial company and whether the investigator has any relationship to the company that owns the digital health technology. Notably, the guidance appears to address both situations in which the technology is the product under study (i.e., the "test article" in the terminology of FDA regulations on clinical investigations) and instances in which the technology is used as a data collection tool but the safety and efficacy of the technology itself is not under study.

- **Component 2: Procedures.** The procedures component describes in more detail how, when and under what circumstances the digital health technology will be used in the research study. For example, this component should describe the types of data that will be shared or submitted to the research study team, instructions on using the study-related digital health technology and how the participant will access the technology (e.g., whether the participant will be required to connect hardware or install software on a personal device), how the participate can stop the sharing and/or collection of data, the frequency of data sharing with or without active participation (e.g., passive collection of heart rate data, location data), how the technology may impact the participant's daily activities, expectations about what participants should not do in relation to the digital health technology during the study and key differences between how the technology is used in the study versus how the technology may be used for general purposes by the public.[6] The procedures component also should inform participants that they must agree to the standard terms and conditions for use of the technology to participate in the study. These generally would be terms of use or end-user license agreements (EULAs) that end users must accept to access a particular digital health tool, such as a mobile application. With respect to third parties, this component also should describe all third parties that may access participant data and whether the shared data may be transmitted to personal health care providers or connected with the

participant's electronic health record (EHR) and the circumstances under which clinically actionable data will be shared. In addition, the procedures component should describe if and when the participant must return any study-provided devices or discontinue any software subscription services upon withdrawal or conclusion of the study.

- **Component 3: Data Sharing and Ownership.** The data sharing and ownership component explains how participant data are collected, stored and shared. This component should describe whether the collected data are confidential or identifiable or associated with "possible stigma," where and how the study team or others store and manage participant data, including the security controls put in place, whether and how data may be shared by the research study team (e.g., with a data repository) or by the company that owns the digital health technology with or without explicit participant consent and for potential future activities and information regarding any EULAs or terms and conditions that participants will need to accept to use the digital health technology for the research study. This component also should inform potential participants about the difference in security protections implemented by the study team as compared to the digital health technology company, if any, and whether the digital health technology may store, collect or display additional information as part of its normal functioning in a manner beyond the scope of the study. In addition, research study teams should consider whether there is a risk of re-identification of participant data, how this may implicate participants' privacy and the confidentiality of their data, and as a result, how the informed consent language should reflect such risk.

- **Component 4: Potential Risks.** The purpose of this component is to communicate clearly how study data are protected, any reasonably foreseeable risks or discomforts related to the use of digital health technologies in the study, including any privacy and security risks (e.g., potential for data breach) and any physical or psychosocial discomfort, and the steps taken by study teams and their institutions to minimize possible privacy risks. For example, this component should address any potential continued data collection after the study ends, if the technology remains on the participant's device or continues to be used by the study participant, potential linking or use of other technologies that may impact access to participant data, the potential risk that the digital health technology may collect information on other individuals (e.g., from the participant's social networks or other surroundings) and potential interference with other technologies that the participant may use on their device. In addition, this component also should describe how the privacy policies or terms and conditions of the company that owns the digital health technology may differ from the research study team's own privacy rules and how updates to software, privacy policies or other terms and conditions during the study period may create additional risk.

- **Component 5: Potential Benefits.** This component of the sample informed consent language should include information regarding any anticipated direct benefits (i.e., not indirect or ancillary benefits) related to participant use of the digital health technology during the research study.

- **Component 6: Cost.** The cost component should describe any potential costs related to use of the digital health technology during the study and who would be responsible for the costs. For example, potential costs may include cellular service or internet connection, subscription payments, maintenance or replacement costs and in-app paid features. This component also should inform participants whether they will incur any costs for continued access to the digital health technology (e.g., via a subscription or other paid access to a software application) after the study ends, if participants wish to continue use.

- **Component 7: Withdrawal.** This component should address how participant data may be used if a participant withdraws from the study or upon study conclusion, whether there are any limitations to data removal upon withdrawal and if the digital health technology will continue to collect data after withdrawal until the technology is removed, uninstalled or otherwise deactivated. The withdrawal component also should clearly establish a protocol and related criteria for formally withdrawing participants for non-adherence to required study activities, which would presumably also include individuals who enroll and are later found not to have met the study's inclusion/exclusion criteria.

Implications for Stakeholders

The Resource provides helpful guidelines for researchers using digital health technologies in their studies. At the same time, researchers must be aware of several other evolving laws and regulations at both the federal and state level that are not discussed in the Resource but that may apply to the use of such technologies. Notably, many of these laws and regulations are enforced by other components of the U.S. Department of Health and Human Services (HHS). We provide a high-level overview of several key relevant authorities here.

Increased Focus on Privacy and Security Issues Related to Digital Health Technologies

The Resource is consistent with the federal government's recent focus on privacy and security issues related to health care-related technologies, including online tracking technologies running on websites and mobile applications, and medical devices in general.

HHS Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) have been particularly active in this area. OCR first released a guidance document in December 2022, which sets forth guidance for HIPAA covered entities and their business associates that utilize online tracking technologies on their patient-facing platforms, and updated the guidance document on March 18, 2024.[7] Specifically, this guidance document describes

how the HIPAA Privacy, Security and Breach Notification Rules apply to HIPAA covered entities' and their business associates' use of tracking technologies, and relatedly, the compliance obligations for such covered entities and their business associates when using tracking technologies. FTC has also released guidance on tracking technologies,[8] and in parallel, initiated enforcement actions against certain companies in connection with unauthorized disclosure of PHI to tracking technology vendors.[9] More recently, on May 30, 2024, FTC published in the *Federal Register* its finalized changes to the Health Breach Notification Rule (HBNR), clarifying that the scope of the rule encompasses health applications and other direct-to-consumer health technologies that are not subject to HIPAA.[10] Heightening the risk in this area, several private plaintiffs have brought class action lawsuits against health care providers under various privacy-related theories related to the collection of health information via online tracking technologies.[11] While not referenced expressly in the Resource, researchers that are part of HIPAA covered entities or business associates, subject to FTC jurisdiction or use a technology subject to the HBNR need to be mindful of how digital health technologies used in their studies comply with the relevant FTC and OCR guidance.

FDA similarly has issued its own guidance related to cybersecurity in medical devices, which in part requires medical device manufacturers to demonstrate reasonable assurance that its medical device and related systems are "cybersecure."[12] In this guidance, FDA also makes recommendations on submission of documentation related to cybersecurity for investigational device exemptions (IDEs). Specifically, FDA recommends that IDE applications should include documentation on the inclusion of cybersecurity risks as part of the informed consent form and general information about connectivity, associated general cybersecurity risks and updateability of the device.[13]

Decentralized Clinical Trials

As discussed above, there has been extensive growth in the use of decentralized clinical trials (DCTs), in particular since the start of the COVID-19 pandemic, both for the investigation of drugs, biological products, and devices, as well as in other types of biomedical and behavioral research. In its draft guidance on DCTs, FDA defines a DCT as "[a] clinical trial where some or all of the trial-related activities occur at locations other than traditional clinical trial sites."[14] DCTs increasingly are being used for clinical trials and other studies because they allow investigators to access a larger sample population, increase clinical trial diversity and conduct real-world analyses. When digital health technologies are used, DCTs can allow for continuous data collection (e.g., via wearables), the ability to document rare events that may not present during traditional clinical trial site visits, and improved participant engagement and adherence.

DCTs utilizing digital health technologies introduce inherent privacy and security risks that research institutions and researchers must consider. In December 2023, FDA issued final guidance on the use of digital health technologies for remote data acquisition in clinical investigations, which provides recommendations for sponsors, investigators and other

stakeholders on using digital health technologies in clinical investigations, and various risk considerations.[15] Related to data privacy and security risks, this FDA guidance document recommends that stakeholders should evaluate the design and operation of the digital health technologies to determine what safeguards are in place to manage privacy and security risks prior to selecting the digital health technology for use in a clinical investigation.[16] FDA also recommends that sponsors planning to use a digital health technology in a clinical investigation should describe in their submissions to FDA "how access to the [digital health technology] or the data collected from it is controlled to ensure privacy and security."[17] As for risks, FDA recommends that sponsors, investigators and IRBs consider:

1. **Clinical risks**, including physical discomfort, risk of physical injury and risk of erroneous measurements resulting in excessive, inadequate or inappropriate treatment;
2. **Privacy-related risks**, including the risk of potential disclosure of personally identifiable information, data sharing with third parties as permitted by EULAs or terms of service (ToS) for the digital health technology, the risk of access by malicious parties, as well as the Secretary's Advisory Committee on Human Research Protections' clarifying requirements on EULAs and ToS in research using digital health technologies; and
3. **Informed consent**, which largely overlap with the considerations outlined in the Resource.[18]

Interaction with Federal and State Privacy and Data Sharing Laws

Many states have enacted data privacy laws that apply to data collected, stored and shared through digital health technologies. Research institutions and researchers that consider use of digital health technologies in their research studies should ensure compliance with applicable state privacy laws and that potential risks related to these state privacy laws are appropriately reflected in informed consent documents. Some state privacy laws may provide exemptions for certain research activities, but these exemptions vary on a state-by-state basis. Therefore, as certain types of research may fall within an exemption in one state, but not in another state, sponsors, research institutions and IRBs should be aware of the relevant state privacy laws that may impact the use of digital health technologies in research. For a nationwide study in which participants will be located in multiple states, study sponsors and investigators may wish to review applicable state laws and conform to the most stringent standard to permit a uniform approach to be taken with respect to all participants. If study participants will be enrolled outside of the U.S., attention will need to be given to ex-U.S. data privacy laws, such as the European Union's General Data Protection Regulation.[19]

Finally, stakeholders must consider the application of federal and state data sharing and interoperability laws and policies, particularly where data are transmitted to participants' personal health care providers, or the technology is connected to EHRs. For example, the

Information Blocking Rule, promulgated by the Office of the National Coordinator for Health Information Technology within HHS, prohibits certain "actors" (health care providers, developers of certified health information technology (HIT) and health information networks and health information exchanges) from engaging in practices that interfere with the access, exchange, or use of electronic health information, except as required by law or permitted by an information blocking exception, as enumerated in the Information Blocking Rule.[20] Clinical research, which may utilize digital health technologies, often involves reviewing clinical data that are stored by health care providers in EHRs or maintained by various certified HIT, which are subject to the Information Blocking Rule. Under the Information Blocking Rule, when researchers request certain electronic health information for research purposes, unless prohibited by law or subject to the specific information blocking exceptions, "actors" are required to provide the requested electronic health information. As another example, the NIH Policy for Data Management and Sharing also may apply to research that utilizes digital health technologies, which requires that researchers develop and submit to NIH data management and sharing plans that outline how scientific data will be managed and shared, including any potential restrictions or limitations on sharing and the reasons therefor.[21]

Conclusion

As digital health technologies continue to permeate the design and focus of research, research institutions, researchers and other stakeholders will have to grapple with various resulting compliance obligations, such as balancing privacy and security risks against data sharing requirements, to reap the benefits of using digital health technologies in research. The Resource provides practical guidelines that should be useful to researchers and their institutions in assessing the use of digital health technologies in studies. Because the Resource understandably cannot address all relevant laws and regulations in this area, researchers and their institutions will need to consider the many other laws, regulations and subregulatory guidance documents that apply to the use of digital health technologies in clinical research.

About the Authors

David Peloquin is a partner in Ropes & Gray's health care group, based in Boston, who advises clients on a wide range of legal and regulatory issues in the area of clinical research, data privacy, provision of health care services and related activities. David guides clients through complex regulatory questions arising under the Common Rule and FDA regulations, data privacy regulations (including HIPAA, U.S. state privacy laws, and GDPR), and state and federal fraud and abuse laws and health care licensing requirements. David is also a member of the firm's digital health practice and frequently advises clients on the use of digital technologies in research and clinical settings. He frequently publishes and speaks on issues related to human subjects research, data privacy and digital health.

Leslie Thornton is counsel in Ropes & Gray's health care group, based in Los Angeles. Leslie advises clients on regulatory and compliance issues related to research and development, including pre-clinical and clinical studies, federal grants and contracts, research misconduct, government enforcement, digital health, and health privacy. Before returning to Ropes & Gray in 2021, Leslie was senior health privacy counsel at Apple Inc., supporting the company's health research initiatives and health-focused teams. With a PhD in public health (psychiatric epidemiology), she understands the day-to-day experience of researchers and research staff, and uses that knowledge base to help her clients find practical solutions to challenging legal and compliance issues.

Carolyn Lye is an associate in Ropes & Gray's health care group, based in Boston. She provides transactional, regulatory, and compliance advice to a broad range of health care clients, including health care providers, academic medical centers, pharmaceutical manufacturers, and investors. Since joining the firm, Carolyn has also co-authored several articles focused on regulatory matters within the health care industry, including on interoperability, information blocking, and drug pricing. Carolyn attended Yale Law School as part of the J.D./M.D. dual degree program, graduating concurrently from Yale School of Medicine in 2022.

---

[1] National Institutes of Technology Office of Science Policy, Informed Consent for Research Using Digital Health Technologies: Points to Consider & Sample Language (May 2024), https://osp.od.nih.gov/wp-content/uploads/2024/05/DigitalHealthResource_Final.pdf.
[2] National Institutes of Technology, "NOT-OD-24-002 – Request for Information: Developing Consent Language for Research Using Digital Health Technologies" (Oct. 11, 2023), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-24-002.html.
[3] The Resources expressly notes that it does not address implantable devices, artificial intelligence, or other types of digital health technologies.
[4] 45 C.F.R. § 46.116; 21 C.F.R. pts. 50 and 56.
[5] National Institutes of Technology, "NOT-OD-21-013 – Final NIH Policy for Data Management and Sharing" (Oct. 29, 2020), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-21-013.html.
[6] Implied, but not expressly stated, in the Resource is the need to inform potential participants regarding what data processing is done *on-device* versus *off-device*, including how and when data move off-device. Oftentimes researchers use on-device data processing as a data privacy protection, to minimize the amount of data leaving the device and, accordingly, to minimize the amount of data received by researchers. This helps to ensure that only those data that are necessary to the research (and approved for collection by participants via the consent process) are received by researchers.
[7] U.S. Department of Health and Human Services Office for Civil Rights, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates" (updated Mar. 18, 2024), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.
[8] Federal Trade Commission, "Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking" (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.
[9] *See, e.g.*, Federal Trade Commission, "FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising" (Feb. 1, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising; Federal Trade Commission, "FTC to Ban BetterHelp from Revealing Consumers' Data, Including Sensitive Mental Health Information, to Facebook and Others for Targeted Advertising" (Mar. 2,

2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-ban-betterhelp-revealing-consumers-data-including-sensitive-mental-health-information-facebook; Federal Trade Commission, "Ovulation Tracking App Premom Will be Barred from Sharing Health Data for Advertising Under Proposed FTC Order" (Mar 17, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/05/ovulation-tracking-app-premom-will-be-barred-sharing-health-data-advertising-under-proposed-ftc.

[10] "Health Breach Notification Rule," 89 Fed. Reg. 47028 (May 30, 2024).

[11] *See, e.g.*, *Santoro v. Tower Health*, Civil Action No. 22-4580, 2024 WL 1773371 (E.D. Pa. Apr. 24, 2024); *Nienaber v. Overlake Hospital Medical Center*, Case No. 2:23-cv-01159-TL (W.D. Wash. May 13, 2024).

[12] U.S. Food & Drug Administration, "Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions" (Sept. 27, 2023), https://www.fda.gov/media/119933/download?attachment.

[13] *Id*. at Appendix 3.

[14] U.S. Food & Drug Administration, "Decentralized Clinical Trials for Drugs, Biological Products, and Devices" (May 1, 2023), https://www.fda.gov/media/167696/download.

[15] U.S. Food & Drug Administration, "Digital Health Technologies for Remote Data Acquisition in Clinical Investigations" (Dec. 2023), https://www.fda.gov/media/155022/download.

[16] *Id.* at 10.

[17] *Id*. at 11.

[18] *Id*. at 18–20.

[19] Regulation (EU) 2016/679.

[20] 45 C.F.R. pt. 171.

[21] National Institutes of Technology, "NOT-OD-21-013 – Final NIH Policy for Data Management and Sharing" (Oct. 29, 2020), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-21-013.html.