Comments of the World Privacy Forum

to the

Department of Health and Human Services, HHS Office for Human Research Protections and the Food and Drug Administration

regarding

Key Information and Facilitating Understanding in Informed Consent; Draft Guidance for Sponsors, Investigators, and Institutional Review Boards; Availability, Docket Number FDA-2022-D-2997

Sent via electronic submission at regulations.gov

Dockets Management Staff (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

April 30, 2024

The World Privacy Forum welcomes this opportunity to comment on the draft guidance from the Department of Health and Human Services and the Food and Drug Administration on *Facilitating Understanding in Informed Consent.* The request appeared in the Federal Register on March 1, 2024, https://www.govinfo.gov/content/pkg/FR-2024-03-01/pdf/2024-04377.pdf. The text of the draft guidance is at https://www.hhs.gov/ohrp/regulations-and-policy/requests-for-comments/draft-guidance-key-information-facilitating-understanding-informed-consent/index.html and https://www.fda.gov/media/176663/download.

The World Privacy Forum (WPF) is a nonprofit, non-partisan 501(c)(3) public interest research group. WPF focuses on multiple aspects of privacy, especially those relating to complex ecosystems, with health privacy being among our key areas of work. We publish a large body of

health privacy information, including guides to HIPAA; reports and FAQs for victims of medical identity theft; and materials on genetic privacy, precision medicine, electronic health records, and more.[1] We testify before Congress and federal agencies, and we regularly submit comments on health privacy regulations. WPF is a special advisor to the board of the World Health Organization's HDC. WPF also serves on a data governance working group at WHO and a GIS working group. You can find out more about our work and see our reports, data visualizations, testimony, consumer guides, and comments at http://www.worldprivacyforum.org.

I. Background discussion

In general, we broadly support the goals of the draft guidance and the proposals included in the draft guidance. We largely agree with the 2018 comments of SACHRP regarding new "Key Information" consent requirements.[2] However, in the comments below, we have made several additional suggestions for improvements in the area of Key Information additions that take into account changes, norms, and laws in today's broader data and data ethics ecosystem. WPF believes that examining consent apart from our current socio-legal-technical data and digital environment has a strong likelihood of leading to potentially poor outcomes due to the many concerns the public has regarding release and extended use of protected health information (PHI). These concerns will need to be more specifically addressed in the new guidance.

In these comments, when we use the term "consent," we are referring to the model of Specific Informed Consent, as discussed in McGuire and Beskow (2010); and Mikkelsen *et al.*(2019); among others.[3] We also note the work of Wiertz *et al* regarding an important analysis of the key consent models today, including Broad Consent, Tiered Consent, Dynamic Consent, Dynamic Specific Consent, and Meta Consent. The authors discuss the ethical benefits and challenges with each model. It is a helpful discussion. There is also a useful discussion of "consent fatigue." In the end, the authors conclude, after analyzing the major consent models:

> "None of the consent models satisfies fully both the demands of the individual rights perspective and of the perspective of research as a public good. Even though Tiered Consent, Dynamic Consent and Meta Consent are designed to fit both perspectives,

---

[1] See World Privacy Forum, *A Patient's Guide to HIPAA*, https://www.worldprivacyforum.org/2019/03/hipaa/. See also our Health Category page for additional materials at https://www.worldprivacyforum.org/category/healthprivacy/.

[2] *SACHRP Commentary on new "key information" Informed Consent Requirements*, HHS, 17 October 2018. https://www.hhs.gov/ohrp/sachrp-committee/recommendations/attachment-c-november-13-2018/index.html

[3] *Specific Informed Consent*, as discussed in the following works: Amy L. McGuire, Laura M. Beskow, *Informed consent in genomics and genetic research*, Annual review of genomics and human genetics. 2010;11:361–381. doi: 10.1146/annurev-genom-082509-141711. *See also*: Rasmus Mikkelsen, Mickey Bjerregaard, et al. *Broad consent for biobanks is best - provided it is also deep*, BMC medical ethics. 2019;20(1):71. doi: 10.1186/s12910-019-0414-6. *See also*: Capron, Alexander Morgan Capron, *Where Did Informed Consent for Research Come From*? The Journal of law, medicine & ethics: a journal of the American Society of Law, Medicine & Ethics 46 (1): 12–29. 2018. doi: 10.1177/1073110518766004.

> they are still met with criticism from both sides. In addition, valid criticisms based on concerns of justice, participation and democratic deliberation, and relational concerns have been levelled at each of the models.
>
> In the light of these criticisms, and given the fact that all these perspectives appear ethically relevant, it becomes impossible to declare one model ethically best under all circumstances. Given the tension of the perspectives of self-determination and medical progress, and given the variety of additional ethical concerns directed at consent models, no consent model can lay claim to be ethically uncontested. Instead, the task at hand is to identify an acceptable compromise, which is to say to balance ethical perspectives."[4]

A comprehensive and state of the art literature review conducted by Kassam *et al* in 2023 found that 71% of participants preferred granular, informative, and transparent consent choices.[5] The study notes that: "76.6% ….of the participants made sharing choices to select at least one PHI value that they would not want to share with a particular researcher. Participants also noted that, if consent choices were not offered, they were less likely to share their PHI."[6] The authors concluded that:

> "There is growing interest in understanding the patient perspective on digital health consent in the context of providing clinical care. There is evidence suggesting that many patients are willing to consent for various purposes, especially when there is greater transparency on how the PHI is used and oversight mechanisms are in place. Providing this transparency is critical for fostering trust in digital health tools and the innovative uses of data to optimize health and system outcomes." [7]

WPF agrees with this statement. The idea of trust in digital ecosystems, particularly digital health ecosystems, is essential. The draft guidance will need to robustly incorporate core ideas that are foundational to privacy and to trustworthy AI. These principles are ensconced in various laws around the world, but exist at their most core expressions in the Fair Information

---

[4] Svenja Wiertz, Joachim Boldt, *Evaluating models of consent in changing health research environments*, Med Health Care Philos. 2022; 25(2): 269–280.
Published online 2022 Mar 14. doi: 10.1007/s11019-022-10074-3 https://link.springer.com/article/10.1007/s11019-022-10074-3.

[5] Iman Kassan, Daria Ilkina, Jessica Kemp et al, *Patient perspectives and preferences for consent in the digital health context: state of the art literature review,* Journal of Medical Internet Research. 2023, Feb 10:25:342507. https://pubmed.ncbi.nlm.nih.gov/36763409/

[6] See note 5.

[7] See note 5.

Practices,[8] The OECD Privacy Guidelines,[9] The OECD Recommendation on AI,[10] and the UNESCO Recommendation on the Ethics of AI,[11] for example. We have noted AI in the consent context quite specifically, and will discuss it a bit more in these comments.

The technical mediation of modern consent is of growing interest today, as noted in the draft guidance. We encourage the FDA and HHS to look at the issues that have arisen in India regarding complex digital consent models at scale. India, with its highly developed real time digital backbone that is fully connected to a biometric identification (Aadhaar ecosystem, or the India stack)[12] is the most populous jurisdiction in the world with an end-to-end digital backbone that is inclusive of full identity data. As such, India is in a unique position and finds itself ahead of the U.S. and other developed nations in regards to digitalization in several sectors, but especially in the financial and the health sectors. Because of this leapfrogged development, India has had more time to experience the reality of digital forms of consent mechanisms in the health and financial sectors at scale. Jain, in his helpful work specific to the health sector, writes that there are legal and ethical challenges in even a very advanced system at scale:

> "In addition to legal challenges, there are ethical implications related to the digitization of healthcare in India. The primary ethical considerations concern the issues of informed consent, and these are critical concerns, particularly important for marginalized persons with low literacy rates, as well as communities that have historically been subject to medical exploitation. For the benefits of digital healthcare to reach those farthest removed from access to quality healthcare, there needs to be a comprehensive data protection and informed consent framework in place."[13]

The understanding of the need for careful balance between the need for acquiring the benefits of digitalization in healthcare and the need for ensuring comprehensive data protection and an informed consent framework in place for all communities including the most vulnerable, is a valuable look at where the tension points are. The U.S. can expect that these or very similar tension points will need to be solved imminently. India is in many respects a "digital canary" due to its advanced digital backbone and highly digitalized healthcare system. It would be wise to heed the lessons learned there as soon as practicable.

---

[8] Robert Gellman, *Fair Information Practices: A basic history*, BobGellman.com, Version 2.22 (Apr. 6, 2022), https://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[9] *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* OECD, (September 23, 1980) https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.

[10] *Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449*, OECD. 2019. https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf

[11] *Ethical Impact Assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence,* UNESCO (2023), https://www.unesco.org/en/articles/ethical-impact-assessment-tool-recommendation-ethics-artificial-intelligence.

[12] The India Stack, https://indiastack.org/.

[13] Dipika Jain, *Regulation of digital healthcare in India: Ethical and legal challenges,* Jindal Global Law School, Healthcare 2023, 11(6), 911. https://doi.org/10.3390/healthcare11060911 .

Our comments in this document are informed by this background information, as well as by our additional work in health privacy ecosystems in the U.S. and elsewhere.

II. Recommendation: Add privacy requirements for researchers and add routine privacy audits for consent(s) given for human subject research

WPF commented extensively on the proposed update to the Common Rule.[14] In our comments, which we filed in 2016, we discussed the need for privacy requirements for health researchers. We also discussed the role of Artificial Intelligence (AI) and machine learning in the 2016 comments, and argued that the imminent impact AI/ML was poised to have on all manner of data, including health data, clinical research, and the health ecosystem generally, deserved meaningful attention in the rule. We knew then from research we had been conducting for WPF's *Scoring of America* report [15] that researchers could not possibly keep up with all of the changes in the data ecosystem that the research for *Scoring of America* had documented. In 2019, we filed additional comments with the NIH requesting that they impose stronger privacy requirements in data sharing agreements, and asked the NIH to impose stronger requirements on researchers. We also requested a small percentage of audits to be conducted in order to add appropriate tension and oversight to the system.

We reaffirm these comments. The need for the original recommendations WPF made is even greater today than when we originally wrote them. We note that a great deal of the health research data in the hands of researchers today is not subject to the privacy or security rules in HIPAA. Indeed, most research data about individuals is not subject to any existing privacy law in the United States. This contrasts with the situation in the European Union and much of the rest of the world, where researchers are generally subject to the same data protection rules as others who process personal data. This very fact causes a loss of patient trust in research and researchers, and could over time contribute to meaningful trust challenges for broader tranches of research.

This brings us to the second reason, which is that some types of research models using AI-infused techniques, or conversely, using large biobanks, may well be finding that informed consent is impossible or nearly impossible. This tends to lead to efforts toward Broad Consent. We believe that further AI use in clinical trials will also lead to additional complexities regarding consent and may require additional and new models for consent. We are considering that one of the issues all of us who care about meaningful consent and health privacy are facing is that it might not be possible to actually make a perfect model for consent. It is going to be important to consider more ecosystem-level improvements to actually get at consent improvements.

---

[14] *Comments of the World Privacy Forum to the Office for Human Research Protections, US Department of Health and Human Services; Department of Education; National Science Foundation, and other agencies regarding Federal Policy for the Protection of Human Research Subjects NPRM, Docket ID HHS OPHS 2015-0008.* World Privacy Forum, 5 January 2016. https://www.worldprivacyforum.org/wp-content/uploads/2016/01/WPF_CommentsNPRM_CommonRule_Jan2016_fs.pdf.

[15] Pam Dixon and Robert Gellman, *The Scoring of America,* World Privacy Forum. April 2014. http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf .

Considering how to change just the consent documents will not get at all of the relevant problems.

For this reason, understanding that the idea of improving consent requires looking at the entire ecosystem of consent, WPF recognizes that another part of this ecosystem includes the researchers themselves. It is not too late for the FDA and HHS to require researchers to abide by a set of privacy rules. This will be important in ensuring that the public trusts researchers and the research they are conducting. As noted in the literature reviews and scholarly literature, the trust of the public is paramount. If the U.S. public were to broadly understand that most clinical research takes place outside of the protections of HIPAA, WPF believes that would be a sizable problem for clinical research. People care about their privacy, and they especially care about their health privacy.

One reasonable and effective response to this concern is to address the need for privacy rules for researchers who are otherwise unconstrained by HIPAA rules. These could begin at a simple level, and progress over time. It is unrealistic to assume, however, that researchers will continue to be left out of privacy rules that now are in place in most jurisdictions for most entities.

III. Recommendation: Add additional required *Key Information* elements to the consent notice regarding plans to share and protect data, and impacts of research outside of the research study

First, WPF agrees that Key Information should be included up front in the consent process.

We have an additional suggestion. In Section C, *Supplemental Information that Could be Included within Key Information,* it was noted that the following information could potentially be added to the Key Information Section of consent notices:

> **"What information about prospective subjects is being collected as part of the research?**
>
> **What are the plans to share and protect data that may be of concern to a prospective subject?**
>
> **What impact will participating in this research have on a prospective subject outside of the research? For example, will it reduce options for standard treatments, prevent prospective subjects from accessing future care or from participating in other studies, or impact personal activities such as driving or sun exposure?"**

WPF urges that these three elements are added to the **Key Information** section of the document as data that must be included in the Key Information section. It is at this point a very poor practice to not inform prospective patients / clinical trial participants of what information is collected as part of the research, and what the plans and promises are regarding both sharing and protecting all of the data. A core aspect of Specific Consent is respect for human autonomy. At this time of digital development, there are not any good policy arguments why globally normative data privacy basics are not provided for in human subject research, which is among the most sensitive of contexts.

WPF believes that to ignore such basic privacy considerations in such an important context can at this point in the highly developed maturity cycle of privacy laws and norms be posited as inappropriate or even unfair, depending on the research project and whether it is simple or complex and what types of information it is collecting.

IV. Recommendation: Clearly and prominently disclose to patients and human research subjects what information is covered under HIPAA, and what information is not covered under HIPAA. Also disclose any privacy law that is applicable to the data.

As mentioned in the previous point, many people in the U.S. do not fully understand that much of the data held in the hands of clinical trial researchers and other medical researchers is not subject to HIPAA. WPF has learned over 20 + years of work in health privacy that the public is greatly confused about the privacy protections available under the federal health privacy rules. As HHS and the FDA know, the HIPAA rules apply only to health care providers, health insurers, and clearinghouses. Some parts of the rule also apply to the Business Associates of these entities.

However, if you ask most individuals and patients how health privacy law works in the U.S., you are likely to be told that HIPAA protects equally all health information no matter who possesses or processes the data. This general lack of understanding regarding the basics of how health privacy works in the U.S. context is a non-trivial impediment to meaningfully informing consumers about health privacy generally and about their health privacy rights under HIPAA specifically. This confusion extends to clinical trials and human subject research, and it is important that all clinical trial participants do not have a fuzzy idea that a health privacy law, somewhere, protects their clinical trial or other health research data.

The depth of the problem regarding public understanding of what is covered and not under HIPAA has been underlined in the past few years by enforcement actions the U.S. Federal Trade Commission has brought against health-related websites and entities. In these cases, the FTC has found that if a statement posted on a non-HIPAA regulated health website uses the term “HIPAA compliant” in a privacy policy or elsewhere, that such a statement may constitute

an unfair and or deceptive act or practice, depending on the context and use case. [16] [17] This is because the term "HIPAA compliant" gives consumers the perception that a website is regulated under HIPAA and therefore confers those protections and rights on their data and activities at the site.[18] The FTC enforcement actions that address the use of "HIPAA-compliant" terminology represent meaningful progress; however, many consumers are still likely to see the term "HIPAA compliant" and mistakenly assume that the business is actually a regulated entity under HIPAA.

Solving the "HIPAA compliance" language problem is not and should not be a goal of the guidance. But the FDA and HHS should take into consideration the HIPAA compliance exemplar, and be aware of the significant depth of privacy law misunderstandings in play. To mitigate this problem in the clinical trial context, people should be clearly told when and if HIPAA protections apply to clinical trials and human subject research, and should be informed of any additional protections available (such as: is there a certificate of confidentiality [19] in place? Is there a state law that would provide additional protections?). Potential participants should also be informed of any potential secondary uses of clinical trial data, including the use of the data for AI model training, or other machine learning training or analysis.

---

[16] The FTC has taken enforcement actions asserting that HIPAA claims may deceive consumers. Key cases include GoodRx, February 2023. See: https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising; and Better Help, July 2023. See: https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter. Additional cases include: Henry Schein, See: https://www.ftc.gov/news-events/news/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled-customers-about-encryption-patient); and SkyMed International, Inc., See: https://www.ftc.gov/news-events/news/press-releases/2020/12/company-provides-travel-emergency-services-settles-ftc-allegations-it-failed-secure-sensitive. Regarding GoodRx, the FTC noted that GoodRx:" …Misrepresented its HIPAA Compliance: GoodRx displayed a seal at the bottom of its telehealth services homepage falsely suggesting to consumers that it complied with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a law that sets forth privacy and information security protections for health data." See: https://www.ftc.gov/news-events/news/press-releases/2023/02/ftc-enforcement-action-bar-goodrx-sharing-consumers-sensitive-health-info-advertising. In the GoodRx complaint, the FTC brought a Count regarding privacy misrepresentation. See Count V, paras 98 - 101. In the BetterHelp FTC complaint, see Section D paras 65 -69 regarding "Respondent's Deceptive HIPAA Seal." See: https://www.ftc.gov/system/files/ftc_gov/pdf/2023169betterhelpcomplaintfinal.pdf.

[17] WPF spoke at the 19 January 2023 FTC Open Commission meeting on the topic of "HIPAA compliant" language. In 2023, just one year's time since WPF made the statement, the FTC has made notable progress in addressing this issue, which is particularly clear in the GoodRx case and the BetterHelp case. See note 3 and 4 below for relevant cases and publications. *2023 WPF Statement to the FTC: Statement of Pam Dixon*, 19 January 2023, FTC Open Commission Meeting, Available at: https://www.worldprivacyforum.org/2023/01/statement-of-pam-dixon-at-the-ftc-open-commission-meeting-regarding-consumer-confusion-around-health-privacy-statements-on-websites/ .

[18] See note 4.

[19] *Certificates of Confidentiality,* National Institutes of Health, https://grants.nih.gov/policy/humansubjects/coc.htm.

An additional issue directly related to privacy misperception problems is that with any health research activity, there are multiple categories of participants. Some may be health care providers subject to HIPAA. Some may be health care providers not subject to HIPAA. Some may be other types of participants who are not subject to HIPAA or to any privacy law or ethical rules at all. We recognize that there may be privacy limits imposed by Institutional Review boards, but those limits may vary considerably from IRB to IRB and from project to project.[20]

Again, to solve the privacy confusion, WPF recommends that research subjects should be expressly told when the HIPAA privacy rule applies to subjects' data and when the HIPAA privacy rule does not apply. For participants not covered by HIPAA, research subjects should be told what privacy rules, if any, apply to those participants.

In offering this suggestion, we are not asking for a lengthy document filled with legal analysis. It would be appropriate to provide a simple explanation when privacy protections do and do not apply, with a clear delineation between those researchers and sponsors covered by HIPAA and not covered by HIPAA. The growing number of state privacy laws may be relevant here, and if those laws apply, they may fill some existing gaps.

V. Challenges with informed consent in today's digital environment, and suggestions for addressing some issues

Obtaining any type of meaningful informed consent today poses many difficulties.

A. Click through training and consent fatigue

For years, websites, apps, and IoT devices have inadvertently trained individuals – and still do so multiple times a day – to simply click through notices of any type and to consent to any terms offered. The option if a person does not click through is a requirement to read multiple pages of mumbo jumbo that many will struggle to read in full, much less understand.

Thus, the easiest course of action, and the one taken by nearly everyone, is to just accept the terms as presented, unread and sight unseen, and click through the document to the next screen. There is nothing truly informed or genuinely consensual about any of this. No matter how one may try to simplify the process and revise the language to be understandable, it will be nearly impossible to overcome training of consumers by websites to simply click any box presented.

We note two challenges here. First, it is becoming increasingly difficult to acquire truly meaningful consent. The literature suggests this is true in the digital context. For example, Gilbert et al in "*Click yes to consent*…" discusses in a small study that web design could slow

---

[20] We note that when HHS revised the Common Rule in 2017, it did not include the proposed standardized privacy safeguards for identifiable private information and identifiable biospecimens. See Final Rule, Federal Policy for the Protection of Human Subjects, 82 Federal Register 7150 (Jan. 19, 2017), https://www.govinfo.gov/content/pkg/FR-2017-01-19/pdf/2017-01058.pdf. In comments soon the proposed revision, WPF strongly supported the idea of mandatory privacy rules for researchers subject to the Common Rule. See https://www.worldprivacyforum.org/2016/01/wpf-files-comments-on-federal-proposal-for-human-subject-research-common-rule.

down the rapid “click through” process for human subject research consent.[21] However, there is an open question about how all types of consent are or are not impacted by digital consent mechanisms and click-throughs.

The second problem relates to consents mediated digitally to people who are vulnerable, poor, inexperienced with technologies, or constrained by an illness or other challenge that prevents full understanding or ability to meaningfully consent. In looking at the digital ecosystem, we note that click-through consents might not be the sole way to perform consent. There should be more work on web design that slows down click-throughs, and there needs to be study of additional approaches.

B. Potential Solutions in the digital context

A simple and effective way to overcome some of the problems associated with consent is to require that each potential research subject for each research project pass a knowledge test based on the consent. The test should be multiple choice and very simple. The test should cover four or five basic points for the research’s objective, benefits, and risks. A passing score should be 100 percent. Finally, each consumer should be allowed to take the same test multiple times until they give proper answers for each question. Learning what the consent form actually says is better than never knowing what it says.

Other ideas for subject testing in conjunction with consent include:

1) The test should be written by someone not involved in the research project;
2) the test should be submitted to and approved by the IRB;
3) HHS and FDA should issue testing guidance and examples for use by the research community; and
4) testing should not be required for research that involves minimal risk.

We note that this testing would also be potentially useful outside of the digital context as well.

VI. Conclusion

In closing, we again note our appreciation for the opportunity to comment on the draft guidance. We stand ready to assist in responding to questions and to generally assist in creating better consents for research.

Respectfully submitted,

Pam Dixon
Executive Director, World Privacy Forum

---

[21] Mark Gilbert, Amanda Bonnell et al, *Click yes to consent: Acceptability of incorporating informed consent into an internet-based testing program for sexually transmitted and blood-borne infections*, International Journal of Medical Informatics, Volume 105. September 2017, Pages 38-48 https://www.sciencedirect.com/science/article/abs/pii/S1386505617301697.