

Exploring Ethics: Understanding the Role of Privacy Policies and IRBs in Digital Health Companies

Jacqlyn Lillie Yourell, Kelsey L McAlister, Clare C Beatty, Jennifer L Huberty

Submitted to: Journal of Medical Internet Research
on: December 30, 2024

Disclaimer: © The authors. All rights reserved. This is a privileged document currently under peer-review/community review. Authors have provided JMIR Publications with an exclusive license to publish this preprint on its website for review purposes only. While the final peer-reviewed paper may be licensed under a CC BY license on publication, at this stage authors and publisher expressly prohibit redistribution of this draft paper other than for review purposes.

Table of Contents

Original Manuscript..... 4

Supplementary Files..... 19

..... 19

Preprint
JMIR Publications

Exploring Ethics: Understanding the Role of Privacy Policies and IRBs in Digital Health Companies

Jacqlyn Lillie Yourell¹ PhD; Kelsey L McAlister¹ PhD; Clare C Beatty¹ MA; Jennifer L Huberty¹ PhD

¹ Fit Minded Inc. Phoenix US

Corresponding Author:

Jacqlyn Lillie Yourell PhD

Fit Minded Inc.

Fit Minded Inc.

Phoenix

US

Abstract

Research efforts are growing rapidly in the digital health industry, but with this growth comes increasing ethical challenges. In this viewpoint paper, we leverage over 20 years of combined experience across academia, industry, and digital health to address critical issues related to ethics, specifically privacy policies and institutional review board (IRB) compliance, which are often misunderstood or misapplied. We examine the purpose of privacy policies and IRBs, provide brief examples where companies faced legal and ethical consequences due to shortcomings, and clarify common misconceptions. Finally, we offer recommendations for digital health companies to improve their ethical practices and ensure compliance in a rapidly evolving landscape.

(JMIR Preprints 30/12/2024:70711)

DOI: <https://doi.org/10.2196/preprints.70711>

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**

Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.

Only make the preprint title and abstract visible.

No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**

Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain visible to all users.

Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <https://preprints.jmir.org/preprint/70711>

No. Please do not make my accepted manuscript PDF available to anyone. I understand that if I later pay to participate in <https://preprints.jmir.org/preprint/70711>

Original Manuscript

Exploring Ethics: Understanding the Role of Privacy Policies and IRBs in Digital Health Companies

Jacqlyn L. Yourell¹, Ph.D., Kelsey L. McAlister¹, Ph.D., M.S., Clare C. Beatty¹, M.A., & Jennifer L. Huberty¹, Ph.D.

¹ Fit Minded, Inc, Phoenix, AZ, United States

Corresponding author:

Jacqlyn Yourell, Ph.D. at Fit Minded, Inc, Phoenix, AZ, U.S.

Phone: (602) 935-6986

E-mail address: jackie@jenhubertyphd.com

Abstract

Research efforts are growing rapidly in the digital health industry, but with this growth comes increasing ethical challenges. In this viewpoint paper, we leverage over 20 years of combined experience across academia, industry, and digital health to address critical issues related to ethics, specifically privacy policies and institutional review board (IRB) compliance, which are often misunderstood or misapplied. We examine the purpose of privacy policies and IRBs, provide brief examples where companies faced legal and ethical consequences due to shortcomings, and clarify common misconceptions. Finally, we offer recommendations for digital health companies to improve their ethical practices and ensure compliance in a rapidly evolving landscape.

Keywords: Digital health; research; industry; ethics

Introduction

There has been rapid growth of research initiatives in commercial settings, with the private sector accounting for over 70% of U.S. research and development expenditures in 2017 [1]. Major companies like Microsoft, Huawei, and Alphabet (Google's parent company) have significantly expanded their involvement in research, co-authoring academic publications and supporting large-scale projects [2]. Between 2012 and 2021, private-sector funding for academic research grew at a faster rate than federal funding [3]. This heightened investment has driven innovation across fields such as digital health, artificial intelligence (AI), and technology.

As private-sector investment in research accelerates, concerns are emerging about whether existing ethical oversight mechanisms are evolving sufficiently to address the complexities of commercial research. A recent paper described how studies involving sensitive data, when conducted without formal ethical review, can lead to public misinformation, erode trust in science, and undermine institutional credibility [4]. These concerns are especially relevant in digital health, where existing company practices and policies—such as internal review processes or general user agreements—may not sufficiently address the ethical complexities of data use and highlights the need for more robust forms of oversight.

Areas like privacy policies and research oversight through Institutional Review Boards have become particularly prominent to better safeguard user data. IRBs are committees that review and monitor research involving human subjects to protect participants' rights and welfare. Trends in ethics for digital health apps are increasingly focusing on data privacy, security, and legal compliance, but ethical concerns are often underemphasized in quality frameworks [5]. For the purpose of this paper, ethics refers to the moral guidelines that researchers follow to ensure they treat participants fairly, respect their rights, and prioritize their well-being in the research

process [6]. Considering the frequent misunderstandings and misapplications of ethical principles—particularly regarding privacy policies and IRBs—the purpose of this paper is to leverage over 20 years of combined experience in academia, industry, and digital health to highlight the importance of complying and integrating ethical practices in commercial settings. As we discuss privacy policies and IRBs in commercial settings, we focus on their purpose, discuss examples where companies have fallen short and faced legal and ethical consequences, and clarify common misconceptions. Throughout this paper, we distinguish between what is legally or procedurally required and what constitutes ethical best practices that go beyond compliance to promote transparency, protect participants, and support responsible research in commercial settings. We conclude with recommendations for digital health companies to enhance ethical practices.

Privacy Policies

Privacy policies play a critical role in digital health research by establishing the framework for how companies handle user data. However, many of these policies fail to adequately address the ethical complexities surrounding data usage for research purposes. While privacy policies are intended to inform users about how their personal data is collected, stored, and shared, they often lack transparency regarding data use for research [7]. Commercial privacy policies may satisfy baseline legal obligations by disclosing practices like data collection, third-party sharing, and data storage. However, they are not federally required to include language that informs users their data may be used to examine user behavior, product effectiveness, or health-related outcomes. As a result, safeguards like obtaining user permission for research or ensuring ethical data use are not legal requirements—they remain ethical responsibilities that companies are encouraged to uphold [8].

When companies overlook ethical considerations in their privacy policies, the consequences can be severe, ranging from legal issues and public backlash to lasting reputational damage. The consequences of inadequate privacy policies can be seen in several high-profile cases. For example, in the Facebook-Cambridge Analytica scandal, users agreed to their data being shared in a privacy policy, but did not fully consent to how that data was sold or used [2]. In this case, Facebook's privacy policy allowed third-party applications to access users' data, but users were unaware that their data would be exploited for political profiling, which led to a significant breach of trust and a \$5 billion fine from the Federal Trade Commission (FTC) [2]. A more recent case involves the meditation app Calm and its use of Twilio, a third-party service, for data collection [9]. Despite Calm's focus on mental wellness, sensitive information about users' mood and mental health shared in the app may have been exposed to other parties through Twilio, highlighting the risks of third-party data handling in digital health contexts [9]. These examples underscore why it is crucial for companies to embed and uphold ethical practices throughout their operations, from product development to data management, ensuring transparency, protecting user rights, and maintaining informed consent.

There are common misconceptions about privacy policies that can lead to serious legal and reputational consequences for companies. The first misconception is that companies can share de-identified research data – data where personal information, such as names or contact details, is removed and cannot be linked to an individual – with third parties without informing users. However, when data is originally collected as part of the business and is later used for research—especially if it includes sensitive information—companies may still need to get user permission or have the data reviewed by an ethics team. This review helps make sure the data has been properly stripped of identifying details, that there is a clear agreement in place about

how a third party can use the data, and that it will be stored and handled securely. Even if a company's privacy policy allows certain uses, relying only on that policy without taking these extra steps can leave gaps in protection and risk losing user trust. The second misconception is that a privacy policy allows a company to use data for any purpose they choose. A privacy policy typically covers how a company collects, uses, stores, and protects user data, as well as details on data sharing, user rights, and how users can control their information. However, it does not generally grant permission for the use of data for research purposes unless explicitly stated and clearly presented to users as "consent." A third misconception is that if a company has a clear privacy policy that states data may be used "for research purposes," then they do not need additional approval to use the data. While a privacy policy that clearly outlines information on using data for research can suffice for consent in some cases, IRB approval is still necessary for publishing in peer-reviewed journals, to maintain compliance with privacy protection laws like HIPAA, and ensure rigorous ethical oversight (See IRB section below).

Institutional Review Board (IRB)

Despite their critical role in ensuring ethical practices, IRBs are often underutilized in commercial settings, leaving gaps in oversight and protection. The IRB reviews research protocols to confirm that using data, whether already collected or not, does not compromise individuals' privacy or safety. The IRB ensures that the research design respects participants' rights, protects individuals, minimizes harm, promotes fairness and supports responsible research practices [10]. IRB approval is not always legally required for company-led research, particularly when the work is not federally funded or regulated. However, review by an ethics board is recommended when the research involves human subjects and is typically required by peer-reviewed journals as a condition for publication [11]. This makes IRB review both an ethical

responsibility and a best practice in responsible research. As digital health companies increasingly conduct and publish research using their customer's data, the need for IRB approval becomes more important.

For example, in 2012, Facebook researchers manipulated the news feeds of nearly 700,000 users to study emotional contagion, altering the content to be more positive or negative and tracking emotional responses through language changes [12]. This experiment was conducted without explicit user consent, relying on broad acceptance of Facebook's general terms of service. While privacy was not the central concern, this study raised significant ethical questions about informed consent and potential psychological harm to participants who unknowingly underwent emotional manipulation. Without IRB oversight, there was no plan to mitigate risk or consideration to the ethical implications of deceiving users [13]. While there were no legal consequences, this resulted in increased ethical scrutiny of Facebook's research practices, changes to its internal review processes, and sparked broader discussions about informed consent and corporate responsibility in digital research. Additionally, the journal where the research was published, *Proceedings of the National Academy of Sciences (PNAS)*, published an editorial expression of concern regarding the lack of informed consent in the study. [14], [15]. While some might argue the study posed minimal risk (unlikely to harm users), IRB involvement would still have required a structured review of those risks, a clear justification for bypassing consent, and safeguards such as informing users afterward (known as debriefing). This case illustrates the real-world consequences of bypassing independent ethical review and highlights how IRBs can proactively address issues of risk, consent, and transparency in digital research.

In another case, researchers scraped and publicly shared sensitive user data from

OkCupid, including personal information and responses to private questions, without obtaining user consent or the platform's approval—violating ethical standards and terms of service [16]. OkCupid filed a DMCA complaint (a legal request to remove copyrighted material), and the data were removed, but it had already been downloaded nearly 500 times, which leaves concerns about future misuse. These cases illustrate the consequences of bypassing independent ethical review and how IRB involvement could have supported more thoughtful risk assessment and ethical planning. Oversight by an IRB could have flagged these ethical concerns early, enforced standards for data handling and consent, and prevented reputational and ethical fallout.

IRBs are often underutilized in digital health largely due to misconceptions, similar to what is seen with privacy policies. First, it is often assumed that IRBs are only necessary for academic research and not for industry-led studies. However, IRBs are an essential part of conducting research using human data, regardless of whether the study is initiated in academia or industry, because IRBs ensure that participants' rights, privacy, and welfare are protected [10]. Second, companies often assume de-identified data does not need IRB approval. In reality, even when personal information has been removed and cannot be linked to individuals, IRB oversight may still be required. The IRB evaluates how the data are anonymized to determine the appropriate level of review needed to protect participant privacy and ensure the research is conducted responsibly. Even when using previously collected de-identified data, IRB review is often recommended to approve the research to ensure the study minimizes risk and protects people's privacy. Third, some companies believe that IRB approval slows company progress towards goals. However, IRBs can actually provide flexibility and help keep costs down by allowing companies to evaluate their products or services more efficiently. For example, companies may submit a broader IRB protocol covering data they regularly collect, which can

reduce delays when analyzing that data for different research questions. This approach allows companies to use their data for various purposes, from investor presentations to peer-reviewed publications. However, this approach relies on what's called broad consent—a general agreement from users that their data may be used for future research. While broad consent may satisfy legal standards in some cases, it still raises ethical concerns about whether users fully understand and agree to how their data might be used—especially when the original context was not research-focused [17]. An IRB helps review whether using the data in this way is appropriate by looking at factors like the company privacy policy and how clearly data use was explained to users.

Recommendations for Digital Health Companies

Below are recommendations to help digital health companies enhance their ethical practices, streamline processes, and protect consumers, which may ultimately enhance company credibility and ensure compliance with ethical standards in research:

1. **Develop an Ethical Research Framework:** Create clear company policies about how data will be used ethically for research. These policies should explain exactly what data will be collected, how it will be used, and how it will be protected. This language can also be used in the IRB application, rather than writing from a blank slate, which can help accelerate the application process. To ensure the company stays on track, regularly review and audit these practices to confirm they continue to align with the policies and meet ethical standards. This proactive approach helps maintain transparency and ensures compliance with legal requirements and recognized standards for the ethical use of human data.
2. **Ensure Clear and Compliant Privacy Policies:** Make sure your privacy policy is accessible, easy for users to understand, and clearly explains how their data will be used,

including for research purposes. The information should be upfront and not buried in complex legal language. Clear, accessible privacy policies that explain how customer data will be handled and used help build trust, foster brand preference, and give companies a competitive edge [18]. Having a scientist and/or legal expert review the policy will help ensure it is accurate and meets ethical and legal standards. A clear and accessible privacy policy can help streamline ethics review by demonstrating that users were made aware of potential research use of their data. In some minimal-risk studies, this can support a request to use the data without requiring individual consent.

3. **Get to Know Commercial IRBs:** When selecting a commercial IRB, consider factors like review timeline, cost, and experience with your type of research. Some commercial IRBs offer faster review processes at higher costs, while others may be more economical but take longer to complete reviews. Research the IRB's reputation and consult with other companies or professionals who have worked with them to ensure you make the best choice for your needs. While commercial IRBs are a good fit for many companies, it is also worth considering alternative models—such as internal ethics boards, academic partnerships, non-profit IRBs, or community-based review panels—which may offer advantages depending on factors like independence, transparency, available resources, and the specific nature of the research.
4. **Integrate IRB Processes into Company Operations and Strategy:** To effectively communicate the importance of IRB approval to executives, it is important to educate them about how it is an essential component of the company's overall operations related to research and data for their competitive advantage. Integrate IRB processes into the company's regular workflow (e.g., develop privacy policies early and have staff who

will handle or interact with customer data complete human subjects training). Explain to executives how this ensures consistent ethical practices and smooth approval processes. This proactive approach can help avoid delays and disruptions in the research cycle. Additionally, emphasize how IRB approval contributes to building credibility with investors, partners, and customers. IRB approval can also protect the company from costly legal issues and reputational damage, improve customer loyalty, attract partnerships, and enhance market positioning [18].

5. **Collaborate with Experts:** Partner with experienced researchers who understand industry-specific IRB requirements to ensure smooth approval processes. These experts can help navigate the nuances of commercial IRBs, meet necessary standards, and avoid delays and rejections. Their guidance on complex issues can save time and resources while ensuring ethical compliance.
6. **Stay Informed and Adaptable:** Stay current with evolving regulations, industry trends, and best practices in research ethics. As laws and standards around data privacy, informed consent, and IRB processes change over time, it is essential for companies to regularly review and update their internal policies to maintain compliance. This proactive approach may help prevent legal issues and costly mistakes while demonstrating the company's commitment to ethical integrity.

Conclusions

Drawing from over 20 years of combined experience in academia, industry, and digital health, we have highlighted a set of key critical ethical considerations that commercial research organizations often overlook. We discussed how ethical considerations are often overlooked in industry, particularly with regard to privacy policies and IRBs, clarifying their function and

benefits for companies. Finally, we provided actionable recommendations for digital health companies to enhance their ethical practices. By adopting these strategies, companies can strengthen their commitment to ethical research, streamline approval processes, and build trust with both consumers and stakeholders, ultimately driving sustainable growth and innovation in the digital health space.

Conflicts of Interest. All authors are employees of Fit Minded, Inc. The views expressed in this manuscript are those of the authors and do not necessarily reflect the official position of Fit Minded, Inc.

References

- [1] R. Mandt, K. Seetharam, C. H. M. Cheng, and R. M. K. S. Cheng and Chung Hon Michael, "Federal R&D funding: the bedrock of national innovation," MIT Science Policy Review. Accessed: Dec. 30, 2024. [Online]. Available: <https://sciencepolicyreview.org/2020/08/federal-rd-funding-the-bedrock-of-national-innovation/>
- [2] "Why commercial investment in university research will only grow," Times Higher Education (THE). Accessed: Dec. 30, 2024. [Online]. Available: <https://www.timeshighereducation.com/hub/huawei/p/why-commercial-investment-university-research-will-only-grow>
- [3] "National Science Board," National Science Board. Accessed: Dec. 30, 2024. [Online]. Available: <http://www.nsf.gov/nsb>
- [4] A. Rajan, "Media dissemination of non-compliant research: Threats to public trust, ethical standards, and systemic integrity," *Asian Bioethics Review*, pp. 1–3, 2025.
- [5] M. M. Zych, R. Bond, M. Mulvenna, J. Martinez Carracedo, L. Bai, and S. Leigh, "Quality Assessment of Digital Health Apps: Umbrella Review," *J Med Internet Res*, vol. 26, p. e58616, Oct. 2024, doi: 10.2196/58616.
- [6] "Ensuring ethical standards and procedures for research with human beings." Accessed: Dec. 30, 2024. [Online]. Available: <https://www.who.int/activities/ensuring-ethical-standards-and-procedures-for-research-with-human-beings>
- [7] M. Srinath, S. Sundareswara, P. Venkit, C. L. Giles, and S. Wilson, "Privacy Lost and Found: An Investigation at Scale of Web Privacy Policy Availability," in *Proceedings of the ACM Symposium on Document Engineering 2023*, Limerick Ireland: ACM, Aug. 2023, pp. 1–10. doi: 10.1145/3573128.3604902.
- [8] E. Vayena and J. Tasioulas, "Adapting Standards: Ethical Oversight of Participant-Led Health Research," *PLOS Medicine*, vol. 10, no. 3, p. e1001402, Mar. 2013, doi: 10.1371/journal.pmed.1001402.
- [9] "Software Used By a Meditation App and DoorDash is Being Sued For Sending Personal Data to Unknown Third Parties Without Consent - Consumer Watchdog." Accessed: Dec. 30, 2024. [Online]. Available: <https://consumerwatchdog.org/privacy/software-used-by-a-meditation-app-and-doordash-is-being-sued-for-sending-personal-data-to-unknown-third-parties-without-consent/>
- [10] C. Grady, "Institutional Review Boards: Purpose and Challenges," *Chest*, vol. 148, no. 5, pp. 1148–1155, Nov. 2015, doi: 10.1378/chest.15-0706.
- [11] "ICMJE | Recommendations | Protection of Research Participants." Accessed: Apr. 03, 2025. [Online]. Available: <https://www.icmje.org/recommendations/browse/roles-and-responsibilities/protection-of-research-participants.html?>
- [12] E. Hu, "Facebook Manipulates Our Moods For Science And Commerce: A Roundup," *NPR*, Jun. 30, 2014. Accessed: Dec. 30, 2024. [Online]. Available: <https://www.npr.org/sections/alltechconsidered/2014/06/30/326929138/facebook-manipulates-our-moods-for-science-and-commerce-a-roundup>
- [13] "Facebook's emotional contagion study and the ethical problem of co-opted identity in mediated environments where users lack control - Evan Selinger, Woodrow Hartzog, 2016." Accessed: Dec. 30, 2024. [Online]. Available: <https://journals.sagepub.com/doi/full/10.1177/1747016115579531>

- [14] “Correction for Kramer et al., Experimental evidence of massive-scale emotional contagion through social networks | PNAS.” Accessed: Dec. 30, 2024. [Online]. Available: <https://www.pnas.org/doi/10.1073/pnas.1412583111>
- [15] “Editorial Expression of Concern: Experimental evidence of massive scale emotional contagion through social networks | PNAS.” Accessed: Dec. 30, 2024. [Online]. Available: <https://www.pnas.org/doi/full/10.1073/pnas.1412469111>
- [16] “Researchers just released profile data on 70,000 OkCupid users without permission | Vox.” Accessed: Dec. 30, 2024. [Online]. Available: <https://www.vox.com/2016/5/12/11666116/70000-okcupid-users-data-release>
- [17] A. M. Froomkin, “Big Data: Destroyer of Informed Consent,” *BIG DATA*, 2019.
- [18] “Customer Data Privacy Practices,” Think with Google. Accessed: Dec. 30, 2024. [Online]. Available: <https://www.thinkwithgoogle.com/future-of-marketing/privacy-and-trust/customer-data-privacy/>

Supplementary Files

Untitled.

URL: <http://asset.jmir.pub/assets/208ed154dfa916120a2f41c3bac2d432.docx>