

Ethical Dimensions for AI - Driven Digital Psychotherapy: Ensuring Data Protection, Safety, and Informed Consent

Dr. Gautham. G MBBS., MD.,

Department of Psychiatry, Sree Balaji Medical College and Hospital, Chennai, India

Email: [gauthamgselvan\[at\]gmail.com](mailto:gauthamgselvan[at]gmail.com)

Abstract: *The integration of artificial intelligence (AI) technologies in digital psychotherapy has revolutionized mental health care, significantly enhancing accessibility and scalability of services worldwide. AI - driven applications offer tailored interventions, real - time monitoring, and personalized support, thereby addressing longstanding challenges such as therapist shortages and geographic barriers. However, alongside these advancements, profound ethical considerations emerge, necessitating careful scrutiny and regulation. This thesis explores the multifaceted ethical dimensions posed by AI in digital psychotherapy, focusing on critical issues of user data protection, safety protocols, accountability, liability frameworks, and informed consent practices. Recent studies indicate a rapid increase in the adoption of AI technologies in mental health interventions, with AI - driven platforms showing promise in improving treatment outcomes and patient engagement. Yet, concerns persist regarding the ethical implications of AI algorithms, including privacy risks associated with data collection and processing. The framework proposed in this thesis aims to provide guidance for responsible AI deployment in psychotherapeutic practices. By synthesizing current research, ethical guidelines, and regulatory insights, this study seeks to foster a balanced approach that maximizes the benefits of AI while mitigating potential risks. It underscores the importance of interdisciplinary collaboration among researchers, clinicians, policymakers, and technologists to develop robust safeguards and ensure ethical integrity in AI - driven mental health care.*

Keywords: Artificial Intelligence (AI), Digital Psychotherapy, Data Protection, Informed Consent, User Safety

1. Introduction

Artificial intelligence (AI) has ushered in a new era in mental health care by enabling the development of AI - driven digital psychotherapy apps [1]. These applications represent a promising solution to longstanding challenges such as limited access to mental health services and the shortage of qualified therapists, particularly in underserved communities and during times of crisis. By leveraging AI technologies, these apps offer scalable and personalized interventions that can adapt in real - time to individual needs, thereby potentially improving treatment outcomes and enhancing patient engagement [2].

Despite their transformative potential, the integration of AI in psychotherapeutic practices raises significant ethical considerations that warrant careful examination. Key concerns include ensuring the privacy and security of sensitive user data, addressing algorithmic biases that could impact treatment recommendations, and determining accountability for decisions made by AI algorithms. Moreover, the shift from traditional therapeutic interactions to automated systems raises questions about the ethical implications of reducing human involvement [3] in mental health care, potentially affecting patient trust and autonomy.

Types of AI - Driven Digital Psychotherapy

In contemporary mental health care, AI - driven digital psychotherapy encompasses a spectrum of innovative approaches aimed at enhancing accessibility and efficacy of treatment interventions. These technologies include machine learning algorithms, natural language processing (NLP), virtual reality (VR), and chatbot interfaces, each presenting unique opportunities and ethical challenges.

Machine learning algorithms play a pivotal role in analyzing vast datasets to personalize treatment recommendations and predict mental health outcomes. However, concerns arise regarding algorithmic biases and the accuracy of these recommendations, as biases inherent in the data used for training can potentially perpetuate disparities in treatment access and outcomes.

Natural language processing (NLP) facilitates interactive communication between users and AI systems, enabling virtual conversations akin to therapeutic dialogues. While NLP enhances user engagement and accessibility by offering real - time support and personalized feedback, ethical considerations revolve around ensuring the confidentiality and privacy of sensitive user information shared during these interactions.

Virtual reality (VR) technologies immerse users in simulated environments designed to evoke therapeutic experiences, such as exposure therapy for anxiety disorders or mindfulness exercises for stress reduction. While VR enhances the effectiveness of psychotherapeutic interventions by providing immersive, controlled environments, ethical challenges include managing user safety and ensuring appropriate therapeutic outcomes without causing undue distress or harm.

Chatbot interfaces represent a form of AI - driven digital psychotherapy that delivers automated responses and support through conversational agents. These chatbots simulate human - like interactions and provide continuous support, particularly beneficial for maintaining engagement and monitoring progress between formal therapy sessions. However, ethical concerns arise regarding the boundaries of AI's capability to effectively address complex emotional and

Volume 13 Issue 7, July 2024

Fully Refereed | Open Access | Double Blind Peer Reviewed Journal

www.ijsr.net

psychological issues, as well as the potential risks of over-reliance on automated systems for mental health support.

Protecting User Data

The protection of user data is a paramount ethical concern in AI - driven digital psychotherapy, particularly given the sensitive nature of personal health data and behavioral patterns. In India, the burgeoning digital health sector necessitates robust strategies and regulatory frameworks to safeguard user information from unauthorized access, data breaches, and misuse. This section explores various methods and regulations in place to protect user data, highlighting challenges and best practices within the Indian context [4].

Regulatory Frameworks in India

India's regulatory landscape for data protection is evolving, with significant steps being taken to establish comprehensive data protection laws. The Personal Data Protection Bill (PDPB) of 2019, which draws parallels to the European Union's General Data Protection Regulation (GDPR), is a crucial legislative effort aimed at protecting personal data. The PDPB mandates data localization, requiring that critical personal data be stored within India, and imposes stringent consent requirements for data collection and processing. Compliance with these regulations is essential for digital psychotherapy apps operating in India.

Strategies for Data Protection

Encryption Techniques:

Encryption is a fundamental technique for ensuring data security. By converting sensitive information into an unreadable format, encryption protects data from unauthorized access during transmission and storage. AI - driven digital psychotherapy apps in India must employ robust encryption standards, such as Advanced Encryption Standard (AES) and RSA encryption, to safeguard user data [5].

Data Anonymization Practices:

Data anonymization involves removing or obfuscating personally identifiable information (PII) to protect user privacy. This practice is crucial for utilizing user data in research and development without compromising individual privacy. In India, anonymization techniques must adhere to guidelines provided by regulatory bodies to ensure compliance and effectiveness.

Secure Data Storage and Access Controls:

Secure data storage solutions, such as cloud - based services with advanced security protocols, are essential for protecting user data. Access controls, including multi - factor authentication (MFA) and role - based access, help restrict data access to authorized personnel only. Implementing these measures reduces the risk of data breaches and unauthorized access [6].

Challenges and Case Studies

Despite advancements in data protection strategies, several challenges persist in maintaining data security and privacy in the context of AI - driven digital psychotherapy:

Data Breaches and Cybersecurity Threats:

The increasing sophistication of cyber - attacks poses a significant threat to data security. In 2020, India witnessed a 37% increase in data breaches [7], underscoring the need for robust cybersecurity measures. Digital psychotherapy apps must invest in advanced threat detection and response systems to mitigate these risks.

User Awareness and Consent:

Ensuring informed consent from users remains a challenge, particularly in a diverse country like India with varying levels of digital literacy. Educating users about data privacy rights and the implications of data sharing is crucial for obtaining genuine consent. Apps should provide clear, accessible information about data practices and user rights [8].

Compliance with Global Standards:

While adhering to local regulations, digital psychotherapy apps must also navigate international data protection standards, such as GDPR, when dealing with cross - border data flows. Achieving compliance with multiple regulatory frameworks requires a nuanced understanding of global data protection laws.

Case Studies:

a) Practo:

Practo, a leading digital health platform in India, has implemented stringent data protection measures, including encryption, anonymization, and secure data storage. Their adherence to data protection regulations and commitment to user privacy serves as a model for other digital health apps.

b) Wysa:

Wysa, an AI - driven mental health app developed in India, employs advanced data security practices to protect user information. By prioritizing user privacy and compliance with global standards, Wysa demonstrates best practices in safeguarding sensitive data.

Best Practices for Data Protection

To ensure robust data protection in AI - driven digital psychotherapy, the following best practices are recommended:

- **Adopt Comprehensive Data Protection Policies:** Develop and implement detailed data protection policies that comply with local and international regulations.
- **Regular Security Audits:** Conduct periodic security audits and vulnerability assessments to identify and address potential weaknesses.
- **User Education and Transparency:** Educate users about their data privacy rights and maintain transparency about data practices.
- **Invest in Advanced Cybersecurity Solutions:** Leverage cutting - edge cybersecurity technologies to detect and mitigate threats proactively.

Protecting User Data

The protection of user data is a paramount ethical concern in AI - driven digital psychotherapy, especially given the sensitive nature of personal health information and behavioral patterns involved. In India, the importance of robust data protection strategies is underscored by the rapid

digitalization of healthcare services and the increasing adoption of AI technologies in mental health care.

Regulatory Frameworks

India is in the process of strengthening its data protection regulations to safeguard user privacy. The proposed Personal Data Protection Bill (PDPB) aims to provide a comprehensive framework for data protection, drawing parallels with international standards such as the General Data Protection Regulation (GDPR) of the European Union. The bill emphasizes consent - based data collection, data minimization, and accountability of data fiduciaries, which are crucial for ensuring the ethical deployment of AI in digital psychotherapy.

Encryption Techniques

Encryption is a fundamental technique to protect user data in digital psychotherapy apps. Implementing end - to - end encryption ensures that data transmitted between users and the AI system remains secure from unauthorized access. In India, leveraging strong encryption protocols is essential given the increasing incidence of cyber threats and data breaches. Encryption not only safeguards user privacy but also builds trust in digital health platforms, encouraging more individuals to seek mental health support [10].

Data Anonymization Practices

Data anonymization is critical for protecting user privacy, especially when data is used for research or training AI algorithms. Anonymization involves stripping personal identifiers from data sets, making it difficult to trace back to individual users. In the Indian context, where data privacy awareness is growing, anonymization practices must be rigorously implemented to prevent misuse of sensitive health information. This is particularly important in a culturally diverse country like India, where stigmatization of mental health issues can deter individuals from seeking help if they fear privacy breaches.

Compliance with International Standards

While India is developing its data protection laws, aligning with international standards such as GDPR can enhance the credibility and security of AI - driven digital psychotherapy platforms. GDPR sets a high bar for data protection, including stringent consent requirements, data subject rights, and data breach notifications. Indian digital health providers adopting similar practices can ensure robust data protection, fostering international collaboration and trust.

Case Studies and Best Practices

Several Indian digital health startups and platforms have adopted best practices in data protection [11]:

YourDOST: A mental health platform that connects users with counselors, YourDOST prioritizes data privacy by implementing strict access controls and encryption protocols. The platform's emphasis on confidentiality has made it a popular choice among Indian users seeking discreet mental health support.

Challenges and Way Forward

Despite these efforts, several challenges remain in protecting user data in AI - driven digital psychotherapy:

- **Regulatory Gaps:** The absence of a finalized and enforceable data protection law in India creates uncertainty and potential loopholes in data privacy practices. The swift enactment and implementation of the PDPB are crucial for addressing these gaps.
- **Public Awareness:** Raising awareness about data privacy and the importance of consent among users is essential. Many individuals in India may not fully understand their rights or the implications of sharing personal health data with digital platforms.
- **Technological Advancements:** As AI and digital health technologies evolve, so do the methods of cyber threats. Continuous updates to encryption and anonymization techniques are necessary to stay ahead of potential breaches.
- **Cross - Border Data Transfers:** With the global nature of AI development and deployment, managing cross - border data transfers while ensuring compliance with varying international regulations remains a complex challenge.

Safety Protocols

Ensuring user safety is paramount in AI - driven psychotherapy apps. Given the sensitivity and complexity of mental health care, implementing comprehensive safety protocols is crucial to protect users from potential harms. This section explores the various measures that can be taken to ensure safety, focusing on risk assessment algorithms, emergency response mechanisms, and user support services. Additionally, ethical considerations in detecting and mitigating potential harms, such as adverse reactions to therapeutic interventions or algorithmic errors, are addressed. The role of human oversight and interdisciplinary collaboration is emphasized to enhance app safety and user well - being, particularly in the Indian context.

Risk Assessment Algorithms

Risk assessment algorithms are designed to evaluate the potential risks associated with users' mental health conditions and the interventions provided by AI - driven psychotherapy apps. These algorithms analyze user data, such as self - reported symptoms and behavior patterns, to identify individuals at risk of severe mental health crises, including suicidal ideation or self - harm [12].

In India, where mental health stigma and lack of access to professional care are significant barriers, AI - driven apps must be equipped with sophisticated risk assessment tools to provide timely interventions. However, the ethical challenge lies in ensuring the accuracy and reliability of these algorithms, as false positives or negatives can have serious consequences. Continuous validation and updating of these algorithms are essential to maintain their effectiveness and safety.

Emergency Response Mechanisms

AI - driven psychotherapy apps must incorporate robust emergency response mechanisms to address situations where users are at immediate risk. These mechanisms can include automated alerts to emergency contacts, real - time connection to crisis helplines, and guidelines for users to follow in critical situations.

In India, the availability of emergency mental health services varies widely across regions. Therefore, apps should be designed to integrate with local crisis response systems, ensuring users can access timely help. Additionally, apps can provide users with information about nearby mental health facilities and support networks, enhancing their ability to seek assistance when needed.

User Support Services

Comprehensive user support services are essential for ensuring the well-being of users interacting with AI-driven psychotherapy apps. These services can include access to trained human counselors, 24/7 helplines, and online support communities. By offering multiple layers of support, apps can provide users with the necessary resources to manage their mental health effectively [13]. In the Indian context, user support services must be culturally sensitive and available in multiple languages to cater to the diverse population. Ensuring that support services are accessible and affordable is also crucial, given the economic disparities that exist within the country [14]. Collaborating with local mental health organizations and leveraging community resources can enhance the effectiveness and reach of these support services.

Ethical Considerations

Several ethical considerations must be addressed to ensure the safety of users interacting with AI-driven psychotherapy apps:

- **Adverse Reactions to Interventions:** AI-driven interventions may not be suitable for all users, and there is a risk of adverse reactions. Continuous monitoring and feedback mechanisms are necessary to detect and mitigate any negative outcomes promptly [15].
- **Algorithmic Errors:** Errors in algorithms, whether due to data quality issues or inherent biases, can lead to incorrect assessments or recommendations. Regular auditing and improvement of algorithms are essential to minimize these risks.
- **Informed Consent:** Users must be fully informed about the potential risks and limitations of AI-driven interventions. Clear communication about the role of AI, the nature of data collection, and the boundaries of the app's capabilities is crucial for maintaining trust and ensuring informed consent.

Role of Human Oversight and Interdisciplinary Collaboration

Human oversight is critical in maintaining the safety and effectiveness of AI-driven psychotherapy apps. Trained mental health professionals should be involved in the development, implementation, and ongoing monitoring of these apps to ensure that they adhere to ethical standards and provide appropriate care.

Interdisciplinary collaboration among technologists, clinicians, ethicists, and policymakers is essential to address the complex challenges associated with AI in mental health care. By working together, these stakeholders can develop comprehensive safety protocols that balance innovation with user protection.

Accountability and Liability

AI-driven psychotherapy apps present complex issues of accountability and liability, involving developers, healthcare providers, and regulatory bodies. This section delves into the responsibilities associated with ensuring app performance, managing algorithmic decisions, and addressing the legal implications of adverse incidents or data breaches. By examining liability frameworks and ethical guidelines, this discussion aims to clarify roles and mitigate legal risks, promoting transparency and accountability in AI-driven mental health interventions, particularly in the Indian context.

Ensuring App Performance

Ensuring the performance of AI-driven psychotherapy apps is a shared responsibility among developers, healthcare providers, and regulatory bodies. Developers must rigorously test and validate their algorithms to ensure they provide accurate and effective therapeutic interventions. Continuous monitoring and updating of these algorithms are necessary to adapt to new data and changing user needs.

In India, where mental health resources are limited, it is crucial that AI-driven apps are reliable and effective. This requires collaboration between developers and mental health professionals to create evidence-based interventions that are culturally relevant and accessible. Regulatory bodies must also establish standards and guidelines for app performance to ensure they meet the necessary therapeutic efficacy and safety requirements.

Managing Algorithmic Decisions

Algorithmic decisions in AI-driven psychotherapy apps must be transparent, explainable, and accountable. Developers are responsible for designing algorithms that are free from biases and errors that could negatively impact users. This includes using diverse and representative datasets during the training phase and implementing mechanisms to detect and correct biases.

Healthcare providers using these apps must understand the underlying algorithms to make informed decisions about their use in clinical practice. In the Indian context, this is particularly important as the population is diverse, and algorithms must be sensitive to cultural, linguistic, and socioeconomic variations. Training programs for healthcare providers on the ethical use and limitations of AI-driven apps can enhance their ability to manage algorithmic decisions responsibly.

Legal Implications and Liability Frameworks

Addressing the legal implications of adverse incidents or data breaches is critical in ensuring accountability in AI-driven psychotherapy apps. In India, the evolving legal landscape, with the introduction of the Personal Data Protection Bill, highlights the importance of stringent data protection measures and clear liability frameworks.

Liability for adverse incidents, such as incorrect treatment recommendations or data breaches, must be clearly defined. Developers, as the creators of the algorithms, hold primary responsibility for ensuring their accuracy and security. Healthcare providers also share liability when they integrate

these apps into their practice, necessitating informed consent and clear communication with users about the app's capabilities and limitations.

Regulatory bodies must establish comprehensive liability frameworks that delineate the responsibilities of all parties involved. These frameworks should include provisions for reporting and addressing adverse incidents, compensating affected users, and imposing penalties for non-compliance. Ensuring that liability is proportionate and fair can encourage innovation while protecting user rights.

Ethical Guidelines

Ethical guidelines play a crucial role in promoting transparency and accountability in AI-driven mental health interventions. These guidelines should address issues such as:

- **Transparency:** Ensuring that users and healthcare providers understand how algorithms work, what data is being collected, and how it is used.
- **Consent:** Obtaining informed consent from users, clearly explaining the potential risks and benefits of using AI-driven psychotherapy apps.
- **Bias and Fairness:** Implementing measures to detect and mitigate biases in algorithms to ensure fair treatment for all users, regardless of their background.
- **Privacy and Security:** Adhering to strict data protection standards to safeguard user information and prevent unauthorized access or breaches.

Promoting Accountability in India

Promoting accountability in AI-driven psychotherapy apps in India requires a concerted effort from all stakeholders:

- **Developers:** Must prioritize ethical considerations in the design and implementation of algorithms, ensuring they are accurate, unbiased, and secure.
- **Healthcare Providers:** Need to be trained in the ethical use of AI-driven apps and should communicate clearly with users about the capabilities and limitations of these technologies.
- **Regulatory Bodies:** Must establish and enforce comprehensive standards and liability frameworks to protect user rights and ensure fair accountability.
- **Users:** Should be educated about their rights and the ethical implications of using AI-driven mental health services, empowering them to make informed decisions.

Informed Consent

Informed consent is foundational to ethical psychotherapeutic practices, and this holds true for AI-driven interventions. In the digital age, obtaining informed consent poses unique challenges, particularly when users interact with AI algorithms instead of human therapists. This section examines these challenges and explores ethical guidelines for disclosing AI capabilities, potential risks, and limitations to empower users in making informed decisions about their mental health care. Strategies for ensuring comprehension, voluntariness, and ongoing consent in dynamic digital interactions are proposed to uphold ethical standards and user autonomy, with a specific focus on the Indian context.

Challenges in Obtaining Informed Consent

Obtaining informed consent in digital environments involves several challenges:

- **Complexity of AI Technologies:** Users may not fully understand how AI algorithms function, their decision-making processes, and the implications of their use in mental health care. This complexity can hinder users' ability to make fully informed decisions.
- **Digital Literacy:** In India, varying levels of digital literacy and access to technology can impact users' ability to comprehend consent forms and the nuances of AI-driven interventions. This is particularly relevant in rural areas and among populations with limited educational backgrounds.
- **Language Barriers:** India is a linguistically diverse country, and providing consent information in multiple languages is essential to ensure comprehension across different linguistic groups.
- **Cultural Sensitivities:** Cultural beliefs and stigmas around mental health can influence users' willingness to seek AI-driven psychotherapy and provide informed consent. Understanding and addressing these cultural factors are crucial for effective consent processes.

Ethical Guidelines for Disclosing AI Capabilities, Risks, and Limitations

To empower users in decision-making, ethical guidelines must be followed to ensure transparency and clarity:

- **Clear Explanation of AI Capabilities:** Users should be provided with a clear and understandable explanation of what the AI-driven app does, how it works, and the nature of the interventions it offers. This includes detailing the role of algorithms in analyzing user data and generating recommendations.
- **Disclosure of Potential Risks:** Users must be informed about the potential risks associated with using AI-driven psychotherapy apps, including data privacy concerns, the possibility of algorithmic errors, and limitations in addressing complex mental health issues.
- **Transparency About Limitations:** It is essential to communicate the limitations of AI-driven interventions, emphasizing that these apps are not substitutes for professional mental health care and should be used as complementary tools.
- **Culturally Sensitive Communication:** Consent forms and information should be tailored to accommodate cultural beliefs and practices, ensuring that users from diverse backgrounds feel respected and understood.

Strategies for Ensuring Comprehension, Voluntariness, and Ongoing Consent

To uphold ethical standards and user autonomy, the following strategies can be implemented:

- **Simplified Consent Processes:** Use simplified language and visual aids to explain AI-driven interventions, making consent forms accessible and understandable for users with varying levels of education and digital literacy.
- **Multilingual Support:** Provide consent information and interfaces in multiple languages to cater to India's diverse linguistic population, ensuring that users can read and understand the information in their preferred language.

- **Interactive Consent Mechanisms:** Develop interactive consent mechanisms, such as videos or interactive tutorials, to enhance users' understanding of the AI - driven app's functionalities and risks.
- **Ongoing Consent:** Implement mechanisms for obtaining ongoing consent, where users are regularly reminded and given the opportunity to reaffirm or withdraw their consent as they continue to use the app. This ensures that users remain informed and autonomous throughout their interaction with the app.
- **User Feedback and Support:** Create channels for users to provide feedback and ask questions about the consent process and the app's functionalities. Offering real - time support through chatbots or human agents can help address users' concerns and enhance their understanding.

2. Conclusions

This thesis concludes by synthesizing key findings and recommendations for the ethical deployment of AI - driven digital psychotherapy apps. Throughout the exploration of various ethical dimensions—including data protection, safety, accountability, liability, and informed consent—it has become evident that a comprehensive and collaborative approach is essential to address these challenges effectively.

3. Key Findings

Data Protection: Ensuring robust data protection through encryption, anonymization, and compliance with regulatory frameworks like the proposed Personal Data Protection Bill in India is critical. Protecting sensitive user information is fundamental to maintaining trust and preventing misuse.

Safety Protocols: Implementing effective safety protocols, such as risk assessment algorithms, emergency response mechanisms, and user support services, is crucial for user well - being. In the Indian context, integrating local crisis response systems and culturally sensitive support services can enhance the efficacy and safety of these apps.

Accountability and Liability: Clear accountability and liability frameworks are necessary to delineate the responsibilities of developers, healthcare providers, and regulatory bodies. Establishing legal standards and ethical guidelines can mitigate legal risks and promote transparency in AI - driven mental health interventions.

Informed Consent: Obtaining informed consent in digital environments requires clear communication, transparency, and strategies to ensure comprehension and voluntariness. In India, addressing digital literacy, language diversity, and cultural sensitivities is essential for effective consent processes.

4. Recommendations for Ethical Deployment

Interdisciplinary Collaboration: Collaboration among researchers, clinicians, policymakers, and technologists is vital to address ongoing ethical challenges. Interdisciplinary efforts can lead to the development of comprehensive

guidelines and standards that balance innovation with user protection.

User - Centric Design: Designing AI - driven psychotherapy apps with a focus on user needs, preferences, and cultural contexts is essential. Involving users in the design process and conducting usability studies can enhance the relevance and accessibility of these technologies.

Continuous Monitoring and Improvement: Regular monitoring and updating of algorithms and safety protocols are necessary to adapt to new data, evolving user needs, and emerging ethical issues. Feedback loops involving users and mental health professionals can help identify areas for improvement.

References

- [1] Smith A. Pew Research Center. Jan 12, 2017. URL: <http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/> [WebCite Cache]
- [2] Gelso CJ, Hayes JA. *The Psychotherapy Relationship: Theory, Research, and Practice*. US: Wiley; 1998.
- [3] Jones N, Moffitt M. Ethical guidelines for mobile app development within health and mental health fields. *Prof Psychol Res Pr*.2016; 47 (2): 155 - 162. [CrossRef]
- [4] Torous J, Roberts LW. Needed innovation in digital health and smartphone applications for mental health: transparency and trust. *JAMA Psychiatry*. May 01, 2017; 74 (5): 437 - 438. [CrossRef] [Medline]
- [5] Giota KG, Kleftras G. Mental health apps: innovations, risks and ethical considerations. *ETSN*.2014; 03 (03): 19 - 23. [CrossRef]
- [6] Nebeker C, Lagare T, Takemoto M, Lewars B, Crist K, Bloss CS, et al. Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Transl Behav Med*. Dec 2016; 6 (4): 577 - 586. [FREE Full text] [CrossRef] [Medline]
- [7] Lang M. Beyond Fitbit: A critical appraisal of optical heart rate monitoring wearables and apps, their current limitations and legal implications. *Albany Law J Sci Technol*. Dec 2017; 28 (1): 39.
- [8] Fisher CE, Appelbaum PS. Beyond Googling: The ethics of using patients' electronic footprints in psychiatric practice. *Harv Rev Psychiatry*.2017; 25 (4): 170 - 179. [CrossRef] [Medline]
- [9] Abril PS, Cava A. Health privacy in a techno - social world: a cyber - patient's bill of rights. *Northwest J Tech Intellect Prop*.2008; 6: 244 - 277.
- [10] Donker T, Petrie K, Proudfoot J, Clarke J, Birch MR, Christensen H. Smartphones for smarter delivery of mental health programs: a systematic review. *J Med Internet Res*. Nov 15, 2013; 15 (11): e247. [FREE Full text] [CrossRef] [Medline]
- [11] Appelbaum PS, Roth LH, Lidz C. The therapeutic misconception: informed consent in psychiatric research. *Int J Law Psychiatry*.1982; 5 (3 - 4): 319 - 329. [Medline]

- [12] Nebeker C, Lagare T, Takemoto M, Lewars B, Crist K, Bloss CS, et al. Engaging research participants to inform the ethical conduct of mobile imaging, pervasive sensing, and location tracking research. *Transl Behav Med.* Dec 2016; 6 (4): 577 - 586. [FREE Full text] [CrossRef] [Medline]
- [13] Böhme R, Köpsell S. Trained to accept? A field experiment on consent dialogs. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.*2010; 4: 2403 - 2406. [CrossRef]
- [14] Cordasco KM. Obtaining informed consent from patients: brief update review. In: *Making Health Care Safer II: An Updated Critical Analysis of the Evidence for Patient Safety Practices.* Rockville, MD. Agency for Healthcare Research and Quality (US); Mar 2013.
- [15] Kreitmair KV, Cho MK, Magnus DC. Consent and engagement, security, and authentic living using wearable and mobile health technology. *Nat Biotechnol.* Jul 12, 2017; 35 (7): 617 - 620. [CrossRef] [Medline]