Journal of AI-Powered Medical Innovations

Volume 1, Issue 1, 2024

Home page https://japmi.org/

Utilizing Artificial Intelligence and Mobile Applications for Mental Healthcare: A Social Informatics Viewpoint

Dr. Alejandro García, PhD

Professor of Biomedical Ethics, Medical University of Lublin, Diagnostic Techniques Unit, Lublin, Poland

The integration of artificial intelligence (AI) and mobile applications into mental healthcare has revolutionized the way individual's access and manage mental health services. This paper examines the intersection of AI technologies, mobile health (mHealth) apps, and mental healthcare through the lens of social informatics. It explores how these technologies influence patient engagement, treatment personalization, and accessibility, while also addressing ethical concerns, data privacy, and the social implications of such advancements. By adopting a social informatics viewpoint, the paper highlights both the potential benefits and challenges that arise from the deployment of AI-powered mobile apps in mental health interventions. The findings aim to inform healthcare practitioners, developers, and policymakers about the future of digital mental healthcare.

Keywords: Artificial intelligence, mobile applications, mental healthcare, social informatics, mHealth, digital health, patient engagement, data privacy, ethical concerns, mental health interventions.

ARTICLE INFO: *Received: 01.08.2024 Accepted: 15.08.2024 Published: 30.08.2024*

INTRODUCTION

This study aims to explore the social implications of using artificial intelligence (AI) in mobile applications for mental healthcare (MHapps). Although there is currently no universally agreed-upon definition of AI (United Nations Economic and Social Commission for Asia and the Pacific and Google, 2019, p. 4), this study will use the definition of AI as "technology designed to perform activities that normally require human intelligence" (Luxton, 2014, p. 332). AI has been used in mental healthcare for decades, and it has the potential to reduce healthcare disparities. However, its current implementations face numerous challenges, including issues of efficacy, privacy, and security, particularly in both clinician-targeted and consumer-marketed MHapps. AI must also be capable of making ethical decisions (Luxton, 2014, p. 336), but it is often hindered by algorithmic biases (Noble, 2018, p. 118; Reidsma, 2016; Whittaker et al., 2018, p. 11). For AI to be implemented effectively and ethically in MHapps, it is essential to examine it through a socially conscious lens at every stage of development, from conception and design to deployment and regulation (Crawford and Calo, 2016, p. 313).

METHODS

A specific type of AI program, chatbots, is commonly included in MHapps. These chatbots, also known as "fully automated conversational agents" (Fitzpatrick et al., 2017; Kretzschmar et al., 2019; Ly et al., 2017), utilize text- or voice-based communication interfaces that mimic human conversation. They are designed to use therapeutic techniques to assist individuals dealing with mental health issues. However, like other AI-driven MHapps, chatbots face similar challenges, including concerns about efficacy and ethical use.

AI and MHapps exist within a broader sociotechnical system, where society and technology mutually influence each other. Social processes are often facilitated by technology, and the societal context can shape how technology is utilized. Ideally, societies should guide technological changes thoughtfully (Kling, 2007, p. 205; MacKenzie & Wajcman, 1999, p. 6). This paper provides an overview of AI and MHapps through a social informatics perspective, examining the development and use of mental health chatbots and other MHapps, and exploring the associated concerns and future potential of these technologies.

DEVELOPMENT OF MOBILE APPLICATIONS FOR MENTAL HEALTHCARE AND ARTIFICIAL INTELLIGENCE CHATBOTS

1. Mobile Applications for Mental Healthcare (MHapps)

The use of the internet to support mental health is a well-established concept, with interventions like e-therapy and online psychoeducational resources having been utilized for many years (Barak et al., 2008, p. 110). MHapps emerged alongside the widespread adoption of mobile devices, and are commonly distributed through app stores, similar to other mobile applications. The integration of AI into MHapps is also not a new phenomenon; as early as 1973, virtual humans were employed to help mitigate suicide risk (Lucas et al., 2014).

2. Development and Use of Artificial Intelligence Chatbots in Mobile Applications for Mental Healthcare

AI chatbot technology dates back to the 1960s, and their inclusion in MHapps has grown steadily over time. Chatbots, sometimes referred to as chatterbots, are AI-driven communication tools designed to simulate human conversation through automated means. Depending on their design, chatbots can interpret written text, emojis, or spoken language (converted into text), analyze the input, and generate an appropriate response (Kretzschmar et al., 2019; Stiefel, 2018). This interaction, where a chatbot receives user input and generates a reply, is known as a conversation. The complexity of these conversations can vary greatly, from simple replies to more sophisticated and nuanced interactions, depending on the underlying technology used to construct the chatbot's responses; more advanced AI systems enable more complex and human-like conversations (D'Alfonso et al., 2017). The selection of technology for a chatbot system is typically aligned with its intended social application.

The conceptual origins of chatbots lie in both psychology and computer science, with early theoretical foundations attributed to Alan Turing's Imitation Game (1950). Formal development of chatbots began around 1966 with the creation of ELIZA by Joseph Weizenbaum, a natural language processing program designed to mimic the empathetic communication style of a clinical psychotherapist (Luxton, 2014, p. 333; Stiefel, 2018). ELIZA was followed in 1972 by PARRY, developed by psychiatrist Kenneth Colby to simulate a paranoid schizophrenic; notably, PARRY and ELIZA even interacted via ARPANET (Cerf, 1973). In 1991, SBAISTO (Sound Blasting Acting Intelligent Text to Speech Operator) was developed with therapist-modeled responses. This was followed in 1995 by ALICE (Artificial Linguistic Internet Computer Entity), which utilized Artificial Intelligence Markup Language (AIML) to facilitate the creation of other chatbots (D'Alfonso et al., 2017; Stiefel, 2018).

Today, chatbots are utilized in various contexts within and beyond e-health, and they are often marketed as alternatives to in-person therapy. MHapps, including those incorporating chatbots, have shown potential in helping patients maintain their mental wellness between in-person visits to mental health professionals, including through psychoeducation (Bakker et al., 2016). Psychoeducation involves providing information about mental health conditions to patients, their families, and caregivers (Rholetter, 2019), which can enhance mental health literacy and potentially reduce stigma (Bakker et al., 2016; Griffiths et al., 2004, p. 347). Overall, psychoeducation is generally associated with positive effects on patients' mental health (Rholetter, 2019). However, the quality and effectiveness of psychoeducation delivered by MHapps are not consistently documented (Breslau and Engel, 2015), and the information provided may not always be suitable for all individuals or be presented in an engaging manner.

CURRENT APPLICATIONS OF MOBILE APPLICATIONS FOR MENTAL HEALTHCARE AND ARTIFICIAL INTELLIGENCE CHATBOTS

1. Demonstrated Need

The mental health field is currently well-positioned for the integration of AI chatbots and other MHapps due to several pressing challenges. Clinicians are often overburdened, clinics are understaffed, and many patients face difficulties in accessing providers' offices (Terry and Gunter, 2018, p. 136). In 2017, the World Health Organization (WHO) reported a global median of just nine mental healthcare workers per 100,000 people, indicating a significant shortage of professionals (Inkster et al., 2018). In the United States, where much of the AI work in MHapps is concentrated, there is a consistent shortage of mental healthcare providers; 60% of US counties lack a psychiatrist (Garg and Glick, 2018). Meanwhile, approximately 20% of Americans experience mental illness, with depression projected to become the leading cause of disease by 2030 (Bakker et al., 2016).

Certain populations, such as sexual and gender minorities (SGM), have an even greater need for mental healthcare but often face stigma and discrimination (SAD) when seeking treatment (Corrigan and Matthews, 2003, p. 241; Gnan et al., 2019; Kidd et al., 2016; Schulman and Erickson-Schroth, 2019). In light of these challenges, MHapps have been promoted as potential solutions to meet the growing demand for mental healthcare. However, these applications are not without flaws; they can exhibit algorithmic biases (Noble, 2018; Whittaker et al., 2018) that may perpetuate the same SAD experienced by marginalized groups.

Recognizing these issues, organizations such as the UK's National Health Service, the Australian Psychological Society, New Zealand's Ministry of Health, and the American Psychiatric Association actively evaluate electronic therapy tools (Rozbroj et al., 2014). Some of these organizations provide lists of recommended MHapps on their official websites; however, these lists are sometimes retracted when problems with the apps arise (Torous et al., 2017, p. 222). While professional associations frequently call for advancements in clinical technologies during their meetings, these appeals are often tempered by official concerns regarding the efficacy, safety, and privacy of MHapps (Stiefel, 2018; Terry and Gunter, 2018, p. 139; Torous et al., 2017, p. 222).

CURRENT APPLICATIONS

One of the most common features of MHapps is the provision of on-demand psychoeducation, which can complement in-person treatment (D'Alfonso et al., 2017, p. 11; Kretzschmar et al., 2019, p. 2). For example, some mental health conditions, such as anxiety (Bakker et al., 2016) and depression (Hickie et al., 2005, p. 201; Hsu et al., 2019), can cause memory loss. On-demand psychoeducation can help individuals experiencing memory loss by allowing them to access information as needed, thereby reducing cognitive load (Bakker et al., 2016; Kuhn et al., 2014, p. 171; Sweller, 2011, p. 71). MHapps deliver psychoeducation through various methods, including chatbots that recognize users' sentiments and provide relevant material based on their emotions (D'Alfonso et al., 2017). Alternatively, chatbots may offer mental health information at set intervals, such as daily check-ins, without analyzing sentiments first.

MHapps can also tailor therapeutic techniques to fit user needs. For instance, these apps can make recommendations based on users' indicated abilities, suggesting activities they can feasibly accomplish (Kuhn et al., 2014, p. 17). This personalized approach is crucial for managing cognitive resources and internal motivation, as individuals with high cognitive resources and motivation are more likely to process information systematically (Lin et al., 2019, p. 280). By tracking which activities a user finds helpful or assessing mood through conversations, AI can make suggestions that align with the user's preferences, potentially boosting motivation. Personalization can encourage continued app engagement, though the techniques embedded in MHapps are not always rigorously tested for efficacy (Griffiths et al., 2004, p. 342; Kretzschmar et al., 2019, p. 5).

MHapps often use push notifications to prompt user engagement, which can enhance adherence (Bakker et al., 2016; Kretzschmar et al., 2019, p. 6). However, excessive notifications can lead to information overload (Wilson, 2001, p. 114) and reduce app usage (Bakker et al., 2016). Information overload may also contribute to Information-Seeking Anxiety (ISA), which arises when there is a gap between what one knows and what one feels they should understand (Wurman, 1989, p. 34). ISA can significantly hinder effective information-seeking (Naveed, 2017). If app users feel overwhelmed, they may experience ISA, which can deter them from navigating mental health information within the app or through other sources.

For individuals who need to regularly track mental health data, such as moods, MHapps and chatbots can document real-time input through automated check-ins (Bakker et al., 2016; Chaudhry, 2016; Fitzpatrick et al., 2017, p. 3; Kretzschmar et al., 2019). Emotion tracking is most effective when conducted at regular intervals and in real-time (Chaudhry, 2016), as this can reduce recall bias that might occur when users log data retrospectively (Bakker et al., 2016). However, the accumulation of such data raises concerns about the privacy and security of users' personal information, as it can include habits, moods, preferred coping mechanisms, and more.

The choice of therapeutic technique significantly impacts the effectiveness of MHapps. Cognitive Behavioral Therapy (CBT), for example, has been effective in both in-person and online settings for reducing anxiety symptoms (Barak et al., 2008, p. 147). MHapps tailored for specific conditions, such as PTSD, can be particularly beneficial. The PTSD Coach app, developed by the U.S. Department of Veterans Affairs, incorporates a distress scale linked to CBT techniques, allows users to connect with support networks, and adheres to stringent security standards. It is designed for use independently or alongside traditional psychotherapy (Kuhn et al., 2014, p. 14). Another example is Ellie, a virtual human psychologist chatbot developed with funding from the U.S. Defense Advanced Research Projects Agency (DARPA). Ellie can build rapport, gather personal information, and identify PTSD symptoms and related issues, such as suicidal ideation, without individuals explicitly disclosing these concerns (Lucas et al., 2014; Molteni, 2017). Combining the mental health literacy content of PTSD Coach with Ellie’s relationship-building capabilities could offer PTSD sufferers a comprehensive suite of therapeutic tools, both for self-help and in conjunction with conventional therapy.

These PTSD-focused apps hold promise, as disclosure of issues like distress and suicidal thoughts in a computerized environment can lead to more honest responses and reduce stigma (Kuhn et al., 2014, p. 12; Lucas et al., 2014, p. 95). The stigma associated with mental illness can be particularly damaging when compounded by stigma related to other aspects of identity, such as the SAD experienced by sexual and gender minorities, racial or ethnic minorities, or those with intersecting marginalized identities (Uldall and Palmer, 2004, p. 12; White and Fontenot, 2019, p. 208). A MHapp may be preferred over other information sources if it provides a sense of privacy and reduces perceived stigma, as mobile devices are viewed as everyday, personal tools. Someone who may hesitate to visit a mental health clinic might feel more comfortable communicating with a chatbot (Kuhn et al., 2014, p. 12). However, stigma can still be perpetuated in AI and other digital platforms due to biased algorithms, which are prevalent in unregulated spaces. Utilizing tools that employ biased algorithms can hinder a person’s ability to find beneficial information and may cause further harm (Noble, 2018, p. 118; Reidsma, 2016).

CONCERNS WITH CHATBOTS AND OTHER MOBILE APPLICATIONS FOR MENTAL HEALTHCARE

1. Lack of Clinical Standards

The integration of AI into e-health represents a significant technical and cultural shift within the mental healthcare field (Crawford and Calo, 2016, p. 313). The relationship between a mental healthcare provider and their patient is critical to creating and sustaining a therapeutic environment (Bakker et al., 2016; Barak et al., 2008, p. 111; Bickmore et al., 2005, p. 21). Similarly, developing a believable and complex conversational style in chatbots can help build user trust (Kretzschmar et al., 2019, p. 3). However, due to the lack of regulation for AI chatbots, this trust can be easily exploited. There is an urgent need for accountability, transparency, oversight, and enforcement of standards to maintain an ethically sound environment for the operation of chatbots in mental healthcare (Whittaker et al., 2018, p. 9). Examining the development of previous e-health tools can guide the responsible use of AI chatbots, ensuring better protection for consumers and their data. Key clinical standards currently lacking for MHapps, including chatbots, are safety, efficacy, and privacy (Kretzschmar et al., 2019). While these technologies hold potential, they should be viewed as part of a broader cultural context; applying new technologies to existing problems does not necessarily resolve the underlying issues (Meyer et al., 2019, p. 309). Efforts must continue to improve the infrastructure and cultural factors that impede mental health treatment. Presently, there are several concerns with AI chatbots that mirror issues seen with other MHapps, as well as problems identified in other sectors using AI, including user-centered design, safety, efficacy, and privacy.

2. User-Centered Design

User-centered design is essential in developing any system, including chatbots. A critical aspect of evaluating MHapps, particularly those incorporating AI, is assessing their suitability for various user groups. Evaluations must consider the technology's intended audience (Noble, 2018, p. 18). For instance, if users display addictive behaviors toward mobile technologies (Terry and Gunter, 2018, p. 136), MHapps that include off-device activities may help mitigate these issues (Bakker et al., 2016). Additionally, some MHapps may not be suitable for groups with specific needs, such as sexual and gender minorities (SGM), who may require therapy that is sensitive to their LGBTQIA identities. Approaches that overlook these factors can cause harm (Rozbroj et al., 2014; Uldall and Palmer, 2004). Without attention to unique user needs, MHapps risk harming the very populations they aim to help or alienating them by failing to provide an informed approach.

Furthermore, an intervention that is effective for one group may not work for another. Once MHapps are available in online marketplaces, users may struggle to identify which interventions are being used and which have been proven effective for their specific concerns. This can hinder consumers from selecting beneficial MHapps. Including links to studies within app descriptions, particularly those that test tools within specific groups, could support informed choices and enhance mental health literacy. However, this requires that such studies be conducted; currently, few MHapps are supported by published evidence. Ultimately, failing to consider the unique needs of a group can result in MHapps that unintentionally harm the populations they are designed to help by not offering an informed therapeutic environment.

3. Safety

Safety is another significant concern with MHapps, particularly in the context of addressing suicidality. Ensuring safety involves providing immediate access to emergency services when a user expresses suicidal ideation. Safety resources must be tailored to the user, such as offering geographically appropriate call centers and direct connections to trusted individuals, including caregivers. Safety is also enhanced by recommending tools and techniques suitable for the individual; as discussed earlier, some therapeutic activities may not be appropriate for all users and could potentially cause harm if used incorrectly.

4. Efficacy

For a MHapp to be considered a clinically effective tool, it must undergo rigorous testing, similar to other therapeutic techniques (Bakker et al., 2016). However, few chatbots have been subjected to clinical testing in randomized control trials, and many MHapps have not been tested at all (Kretzschmar et al., 2019; Terry and Gunter, 2018, p. 139). Some chatbots, such as Shim, Wysa, and Woebot, have undergone limited testing (Fitzpatrick et al., 2017; Inkster et al., 2018; Kretzschmar et al., 2019; Stiefel, 2018). These studies have shown some positive effects, including reductions in depression and anxiety symptoms for Woebot users (Fitzpatrick et al., 2017), improvements in depressive symptoms for Wysa users (Inkster et al., 2018), and stress reduction for Shim users (Ly et al., 2017, p. 10). However, these studies often face significant limitations, such as small sample sizes and a lack of comparisons to face-to-face therapy.

As previously noted, some MHapps, like Therachat, lack published clinical studies, highlighting a common gap in the testing of many chatbots and other MHapps. The efficacy of these tools also depends on the therapeutic techniques they incorporate. Cognitive Behavioral Therapy (CBT) is a well-documented treatment for anxiety and depression, proven effective both in-person and online (Bakker et al., 2016). Many MHapps, including Shim, Wysa, and Woebot, utilize CBT. Psychoeducation, an integral part of CBT, should be systematically evaluated for quality and efficacy before inclusion in a MHapp (Hoffman, 2006, p. 469). Thus, the efficacy of a MHapp should be assessed based on the entire app, rather than individual components.

While app creators often highlight the potential benefits of MHapps, clinicians are unlikely to recommend them without solid evidence of their efficacy. Currently, the scarcity of empirical studies on MHapps means that evidence-based guidelines and recommendations cannot be established for many of these tools, including chatbots (Torous et al., 2017). Nevertheless, due to the growing demand for MHapps, some professional organizations have developed evaluation models. For instance, the American Psychiatric Association's (APA) App Evaluation Model provides a framework for clinicians to use when discussing MHapps with patients. The APA's guidelines involve five steps: collecting basic information about the app, examining its privacy and safety features, evaluating its efficacy, assessing user-friendliness, and reviewing data-sharing capabilities. The APA emphasizes that because MHapps are constantly evolving, having flexible guidelines rather than a fixed rating or recommendation system better serves the needs of the mental health community (American Psychiatric Association, 2018). However, even with published assessment frameworks, there is no guarantee that MHapps will incorporate evidence-based recommendations (Bakker et al., 2016), especially as adherence to these guidelines is not mandatory.

The lack of demonstrated efficacy among MHapps contributes to information overload in the marketplace. MHapps may be marketed and sold without clear evidence of safety or effectiveness, making it difficult for consumers to discern these gaps. Ethical clinicians typically rely on evidence-based practices before implementing therapeutic tools, but general users may struggle to distinguish between tested and untested MHapps or to understand the implications of these distinctions. In fact, many MHapps that have been clinically tested and discussed in published studies are not available for public download through major platforms like Apple or Google (Torous et al., 2017). Addressing efficacy concerns could benefit from the AI Now 2018 Report's call for greater transparency (Whittaker et al., 2018); clearer, consumer-focused information about what MHapps offer could help users make more informed choices.

5. Privacy

In addition to concerns about efficacy, privacy regulations for chatbots in mental healthcare (MHapps) are a significant issue. When Woebot was released, the chair of the APA's smartphone app evaluation working group raised concerns about the program's ability to maintain client confidentiality (Stiefel, 2018), concerns which remain unaddressed. AI technologies, including chatbots, have the potential to cause significant harm concerning the privacy of personal healthcare data (Whittaker et al., 2018). MHapp chatbots often collect intimate health information from users who typically expect their data to remain private. Many of these apps also track location data, permit audio recording, and may be linked to financial information, resulting in databases containing extremely sensitive personal data. However, this information is often not governed by regulations that typically protect health data, such as the Health Insurance Portability and Accountability Act (HIPAA) (Stiefel, 2018; Terry and Gunter, 2018).

Privacy concerns are especially critical in MHapps due to the stigmatization associated with mental illness (Koffi et al., 2018, p. 4). People seeking mental health care must trust that their privacy will be protected to minimize fears of stigmatization. Due to this stigma, individuals may feel more comfortable disclosing issues to a chatbot (Lucas et al., 2014, p. 95; Molteni, 2017); for example, virtual human-like tools such as Ellie can detect PTSD symptoms in otherwise reluctant individuals, and chatbots like Woebot can help teenagers disclose suicidal ideation. However, if users do not believe their privacy is protected, they may fear stigmatization and refrain from disclosing sensitive information to the MHapp. Consequently, perceived or actual privacy breaches can undermine the efficacy of these tools.

Users may assume that chatbots are medical mental health tools, especially when MHapps market themselves as companions or alternatives to talk therapy, which is inherently private. However, a 2018 legal study by Scott Stiefel found that chatbots have minimal regulations governing privacy. In the U.S., the Food and Drug Administration (FDA) does not currently classify chatbots as medical devices, leaving them outside the scope of FDA regulation. When chatbots are positioned as self-help tools rather than medical devices, the information shared is not protected by confidentiality regulations. No state laws specifically cover confidentiality in chatbots, and the only privacy requirement is that chatbots notify users of data disclosures, not that they prevent them. This regulatory gap leaves user data vulnerable. At the very least, users should be clearly informed about what data is being collected, how it is used, and what protections, if any, are in place (Whittaker et al., 2018). Privacy policies on MHapp websites can be helpful, but the information should also be presented within the app in an accessible, user-friendly format.

For in-person patient data, HIPAA safeguards privacy. For chatbots like Therachat, which share patient conversations with clinicians, or MHapps like Recovery Record that connect patient logs with mental health providers, HIPAA applies (Recovery Record Inc, 2019; Therachat, n.d.). However, Stiefel notes that HIPAA only covers healthcare providers who bill insurance (2018). Consequently, chatbots operate in a space where users may confide in them as they would with a therapist, but without the same confidentiality protections, and potentially without users being aware that their information is not private. This lack of regulation means that chatbots could use data in various unexpected ways, such as creating targeted marketing or selling the information to third parties (Nissenbaum, 2011; Stiefel, 2018). Such unauthorized use violates the Electronic Privacy Information Center's Code of Fair Information Practices (Electronic Privacy Information Center, n.d.). While some MHapps, like Woebot and Wysa, claim to anonymize and not share user data, other MHapps do not incorporate these protections (Kretzschmar et al., 2019). Users may cease using a chatbot that discloses their personal information, similar to how individuals abandon social media platforms after data breaches, but others may rely on the chatbot and feel unable to discontinue its use.

Ultimately, mental health treatment hinges on maintaining patient confidentiality, including client–therapist privilege (Koffi et al., 2018; Stiefel, 2018; Terry and Gunter, 2018, p. 141). Currently, U.S. laws do not recognize MHapps, including chatbots, as mental health providers or medical devices. Therefore, information shared with a chatbot, even if the user views the chatbot as a virtual therapist, is not considered confidential (American Psychiatric Association, 2018; Stiefel, 2018). If users are unaware of the terms governing their interactions with chatbots and have incorrect expectations of privacy, this could lead to a breach of trust in the MHapp. Such breaches can lead to disuse of the tool, potentially damaging the user's confidence in other MHapps and even traditional mental health treatments.

Additional privacy concerns arise when a MHapp connects to or operates through another platform, such as a social media site. For instance, some MHapps allow users to log in through social media accounts for account creation and synchronization (Bakker et al., 2016). Others, like Woebot, are available as standalone apps or via platforms like Facebook Messenger. In these cases, the privacy standards of the communication platform, not the MHapp, apply (Stiefel, 2018). For example, when using Woebot on Facebook Messenger, Facebook's privacy policies take precedence, allowing Facebook to share user information with third parties (Kretzschmar et al., 2019). From a privacy standpoint, it is safer for MHapp chatbots to have separate, anonymized mobile interfaces to protect users. By providing a secure and private space for discussing mental health concerns, AI chatbots can adhere to ethical guidelines, fostering trust and encouraging greater use of these tools.

LIMITATIONS AND FUTURE DIRECTIONS

This study was limited by its approach as a scoping literature review rather than a systematic review. The informal documentation of the literature searches and the reliance on the judgment of a single researcher for the inclusion of references further constrained the study. A future systematic review would fully document the searches and apply formal inclusion criteria using the Grading of Recommendations, Assessment, Development, and Evaluations (GRADE) framework (Guyatt et al., 2011). Additionally, at least one additional researcher would evaluate references against these criteria to determine inclusion in the systematic review. This study also focused on English-language MHapps available in the USA. Future research could expand to examine the use of MHapps in other countries and languages, offering a global perspective on AI in MHapps, particularly with regard to ethics and regulations.

CONCLUSION

1. Avoiding Techno-Fundamentalism

Dr. Safiya Noble highlighted that Google search results can return biased information that perpetuates racist and sexist depictions of women of color (2018). Similar algorithmic biases have been identified in other electronic platforms, including library discovery tools (Reidsma, 2016). These biases also exist in MHapps, including AI chatbots. If a chatbot operates within a black box, where its underlying algorithms and data are not accessible, it poses a potential danger to those seeking mental healthcare (Whittaker et al., 2018, p. 11). To prevent bias and harm, AI chatbots should adhere to standards established by organizations such as the AI Now Institute, APA, and the Electronic Privacy Information Center.

While MHapps and AI chatbots are designed to help people, there is a clear need for support in mental healthcare due to the shortage of mental health clinicians, especially in underserved areas. This shortage disproportionately affects individuals with lower incomes, including adolescents, the elderly, ethnic and racial minorities, sexual and gender minorities (SGM), and other vulnerable populations. Stigma surrounding mental health further discourages individuals from seeking clinical help. Although MHapps and AI chatbots have the potential to address some of these gaps in mental healthcare, concerns about user-centered design, efficacy, safety, and privacy make them a precarious solution. These tools are intended to complement, not replace, therapy and other mental healthcare, often operating within a clinician-led environment or as self-help activities. However, media portrayals can sometimes misleadingly suggest that chatbots are complete solutions for complex mental health issues (Molteni, 2017). Transparent advertising by vendors and consumer protection agencies can reduce the risk of exploitation of vulnerable populations (Whittaker et al., 2018, p. 5). Ethical operation of AI chatbots requires honest marketing as a baseline standard.

AI chatbots collect substantial amounts of user data to enhance their self-help capabilities. For some chatbots, this information can be shared with the user's clinician, potentially offering HIPAA protections. However, other chatbots operate outside such regulations, risking privacy and security breaches. These chatbots should clearly communicate their limitations, including what data is collected, how it is used, and how it is protected, to safeguard user information. Ensuring data security is crucial from both a therapeutic and ethical standpoint.

Individuals with mental illness often require ongoing, in-person treatment from a variety of clinicians throughout their lives. Depending on the type and severity of their conditions, they may experience a range of outcomes, including institutionalization, unemployment, or leading productive and healthy lives. While AI chatbots can provide tools, forums for discussion, mood tracking, and psychoeducation, they cannot replace therapists. Unlike psychiatrists, AI cannot prescribe lifesaving medications. AI should be viewed as a component of a broader sociotechnical system, not a complete solution. For AI chatbots and MHapps to have a meaningful positive impact, they must be regulated, and society must avoid falling into techno-fundamentalism regarding AI for mental health.

REFERENCES

[1]. Gupta, A., & Agarwal, P. (2024, May). Enhancing Sales Forecasting Accuracy through Integrated Enterprise Resource Planning and Customer Relationship Management using Artificial Intelligence.

In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-6).IEEE.

[2]. Agarwal, P., & Gupta, A. (2024, May). Cybersecurity Strategies for Safe ERP/CRM Implementation.In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-6).

IEEE.

[3]. Gupta, A., & Agarwal, P. (2024, May). Enhancing Sales Forecasting Accuracy through IntegratedEnterprise Resource Planning and Customer Relationship Management using Artificial Intelligence. In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (pp. 1-6).IEEE.

[4]. Patibandla, K. R. (2024). Automate Amazon Aurora Global Database Using Cloud Formation. *Journalof Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *2*(1), 262-270.

[5]. Patibandla, K. R. (2024). Design and Create VPC in AWS. *Journal of Artificial Intelligence Generalscience (JAIGS) ISSN: 3006-4023*, *1*(1), 273-282.

[6]. Abbasi, N. (2024). Artificial Intelligence in Remote Monitoring and Telemedicine. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *1*(1), 258-272.

[7]. Abbasi, N., Nizamullah, F. N. U., Zeb, S., Fahad, M., & Qayyum, M. U. (2024). Machine Learning Models for Predicting Susceptibility to Infectious Diseases Based on Microbiome Profiles. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, *3*(4), 35-47.

[8]. Zeb, S., Fnu, N., Fahad, M., Qayyum, M. U., & Abbasi, N. (2024). Enhancing Diagnostic Accuracy for Medical Imaging and Radiology with AI-Driven Synergy Tools: Enabling Early Intervention and Preventive Measures through Early Detection of Cardiovascular Conditions. *European Journal of Science, Innovationand Technology*, *4*(4), 38-47.

[7]. Abbasi, N., & Hussain, H. K. (2024). Integration of Artificial Intelligence and Smart Technology: AI-Driven Robotics in Surgery: Precision and Efficiency. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *5*(1), 381-390.

[8]. Abbasi, N., Nizamullah, F. N. U., Zeb, S., & Fardous, M. D. (2024). GENERATIVE AI IN HEALTHCARE: REVOLUTIONIZING DISEASE DIAGNOSIS, EXPANDING TREATMENT OPTIONS,

AND ENHANCING PATIENT CARE. *Journal of Knowledge Learning and Science Technology ISSN:2959-6386 (online)*, *3*(3), 127-138.

[9]. Weng, Y., & Wu, J. (2024). Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *5*(1), 392-399.

[10]. Islam, M. M. (2024). Cognitive Frameworks for Mitigating Antiblack Bias: Advancing Ethical AI Design and Development. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *4*(1), 1-12.

[10]. Suryadevara, S., & Yanamala, A. K. Y. (2020). Fundamentals of Artificial Neural Networks: Applications in Neuroscientific Research. *Revista de Inteligencia Artificial en Medicina*, *11*(1), 38-54.

[11]. Yanamala, A. K. Y. (2022). Cost-Sensitive Deep Learning for Predicting Hospital Readmission: Enhancing Patient Care and Resource Allocation. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 56-81.

[12]. Suryadevara, S. (2022). Real-Time Task Scheduling Optimization in WirelessHART Networks: Challenges and Solutions. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 29-55.

[13]. Suryadevara, S. (2022). Enhancing Brain-Computer Interface Applications through IoT Optimization. *Revista de Inteligencia Artificial en Medicina*, *13*(1), 52-76.

[14]. Yanamala, A. K. Y., & Suryadevara, S. (2022). Adaptive Middleware Framework for Context-AwarePervasive Computing Environments. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *13*(1), 35-57.

[15]. Suryadevara, S., Yanamala, A. K. Y., & Kalli, V. D. R. (2021). Enhancing Resource-Efficiency and Reliability in Long-Term Wireless Monitoring of Photoplethysmographic Signals. *International Journal ofMachine Learning Research in Cybersecurity and Artificial Intelligence*, *12*(1), 98-121.

[16]. Suryadevara, S. (2021). Energy-Proportional Computing: Innovations in Data Center Efficiency andPerformance Optimization. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 44-64.

[17]. Suryadevara, S., & Yanamala, A. K. Y. (2021). A Comprehensive Overview of Artificial Neural Networks: Evolution, Architectures, and Applications. *Revista de Inteligencia Artificial en Medicina*, *12*(1),51-76.

[18]. Yanamala, A. K. Y., Suryadevara, S., & Kalli, V. D. R. (2024). Balancing Innovation and Privacy: TheIntersection of Data Protection and Artificial Intelligence. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *15*(1), 1-43.

[19]. Yanamala, A. K. Y., & Suryadevara, S. (2024). Emerging Frontiers: Data Protection Challenges and Innovations in Artificial Intelligence. *International Journal of Machine Learning Research in Cybersecurityand Artificial Intelligence*, *15*(1), 74-102.

[20]. Yanamala, A. K. Y., & Suryadevara, S. (2024). Navigating Data Protection Challenges in the Era of Artificial Intelligence: A Comprehensive Review. *Revista de Inteligencia Artificial en Medicina*, *15*(1), 113-146.

[21]. Yanamala, A. K. Y. (2024). Optimizing Data Storage in Cloud Computing: Techniques and Best Practices. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 476-513.

[22]. Yanamala, A. K. Y. (2024). Emerging Challenges in Cloud Computing Security: A Comprehensive Review. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4), 448-479.

[23]. Yanamala, A. K. Y., Suryadevara, S., & Kalli, V. D. R. (2023). Evaluating the Impact of Data Protection Regulations on AI Development and Deployment. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(01), 319-353.

[25]. Yanamala, A. K. Y. (2023). Data-driven and artificial intelligence (AI) approach for modelling andanalyzing healthcare security practice: a systematic review. *Revista de Inteligencia Artificial en Medicina*, *14*(1), 54-83.

[26]. Yanamala, A. K. Y., & Suryadevara, S. (2023). Advances in Data Protection and Artificial Intelligence: Trends and Challenges. *International Journal of Advanced Engineering Technologies andInnovations*, *1*(01), 294-319.

[27]. Maddireddy, B. R., & Maddireddy, B. R. (2020). Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment. *International Journal of Advanced Engineering Technologies andInnovations*, *1*(2), 64-83.

[28. Maddireddy, B. R., & Maddireddy, B. R. (2021). Evolutionary Algorithms in AI-Driven Cybersecurity Solutions for Adaptive Threat Mitigation. International Journal of Advanced Engineering Technologies andInnovations, 1(2), 17-43.

[29]. Maddireddy, B. R., & Maddireddy, B. R. (2020). AI and Big Data: Synergizing to Create Robust Cybersecurity Ecosystems for Future Networks. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 40-63.

[30]. Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *International Journal of Advanced Engineering Technologiesand Innovations*, *1*(2), 270-285.

[31]. Maddireddy, B. R., & Maddireddy, B. R. (2022). Real-Time Data Analytics with AI: Improving Security Event Monitoring and Management. *Unique Endeavor in Business & Social Sciences*, *1*(2), 47-62.

[32]. Maddireddy, B. R., & Maddireddy, B. R. (2022). AI-Based Phishing Detection Techniques: A Comparative Analysis of Model Performance. *Unique Endeavor in Business & Social Sciences*, *1*(2), 63-77.

[33]. Maddireddy, B. R., & Maddireddy, B. R. (2022). Blockchain and AI Integration: A Novel Approach to Strengthening Cybersecurity Frameworks. *Unique Endeavor in Business & Social Sciences*, *1*(2), 27-46.

[34]. Maddireddy, B. R., & Maddireddy, B. R. (2021). Enhancing Endpoint Security through Machine Learning and Artificial Intelligence Applications. *Revista Espanola de Documentacion Cientifica*, *15*(4),154-164.

[35]. Maddireddy, B. R., & Maddireddy, B. R. (2022). Cybersecurity Threat Landscape: Predictive Modelling Using Advanced AI Algorithms. *International Journal of Advanced Engineering Technologiesand Innovations*, *1*(2), 270-285.

[36]. Maddireddy, B. R., & Maddireddy, B. R. (2023). Automating Malware Detection: A Study on the Efficacy of AI-Driven Solutions. *Journal Environmental Sciences And Technology*, *2*(2), 111-124.

[37]. Maddireddy, B. R., & Maddireddy, B. R. (2023). Enhancing Network Security through AI-Powered Automated Incident Response Systems. *International Journal of Advanced Engineering Technologies andInnovations*, *1*(02), 282-304.

[38]. Maddireddy, B. R., & Maddireddy, B. R. (2023). Adaptive Cyber Defense: Using Machine Learning toCounter Advanced Persistent Threats. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(03), 305-324.

[39]. Maddireddy, B. R., & Maddireddy, B. R. (2024). Neural Network Architectures in Cybersecurity: Optimizing Anomaly Detection and Prevention. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 238-266.

[40]. Maddireddy, B. R., & Maddireddy, B. R. (2024). A Comprehensive Analysis of Machine Learning Algorithms in Intrusion Detection Systems. *Journal Environmental Sciences And Technology*, *3*(1), 877-891.

[41]. Maddireddy, B. R., & Maddireddy, B. R. (2024). The Role of Reinforcement Learning in Dynamic Cyber Defense Strategies. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 267-292.

[42]. Maddireddy, B. R., & Maddireddy, B. R. (2024). Advancing Threat Detection: Utilizing Deep LearningModels for Enhanced Cybersecurity Protocols. *Revista Espanola de Documentacion Cientifica*, *18*(02), 325-355.

[43]. Nalla, L. N., & Reddy, V. M. (2020). Comparative Analysis of Modern Database Technologies inEcommerce Applications. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 21-39.

[44]. Reddy, V. M., & Nalla, L. N. (2020). The Impact of Big Data on Supply Chain Optimization in Ecommerce. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 1-20.

[45]. Nalla, L. N., & Reddy, V. M. (2021). Scalable Data Storage Solutions for High-Volume E-commerceTransactions. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(4), 1-16.

[46]. Nalla, L. N., & Reddy, V. M. (2022). SQL vs. NoSQL: Choosing the Right Database for Your Ecommerce Platform. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2),54-69.

[47]. Reddy, V. M., & Nalla, L. N. (2022). Enhancing Search Functionality in E-commerce with Elasticsearch and Big Data. *International Journal of Advanced Engineering Technologies andInnovations*, *1*(2), 37-53.

[48]. Reddy, V. M., & Nalla, L. N. (2021). Harnessing Big Data for Personalization in E-commerceMarketing Strategies. *Revista Espanola de Documentacion Cientifica*, *15*(4), 108-125.

[49]. Reddy, V. M., & Nalla, L. N. (2024). Real-time Data Processing in E-commerce: Challenges and Solutions. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 297-325.

[50]. Reddy, V. M., & Nalla, L. N. (2024). Leveraging Big Data Analytics to Enhance Customer Experiencein E-commerce. *Revista Espanola de Documentacion Cientifica*, *18*(02), 295-324.

[51]. Reddy, V. M., & Nalla, L. N. (2023). The Future of E-commerce: How Big Data and AI are Shapingthe Industry. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(03), 264- 281.

[52]. Pureti, N. (2020). The Role of Cyber Forensics in Investigating Cyber Crimes. *Revista de InteligenciaArtificial en Medicina*, *11*(1), 19-37.

[53]. Pureti, N. (2020). Implementing Multi-Factor Authentication (MFA) to Enhance Security. *InternationalJournal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *11*(1), 15-29.

[54]. Pureti, N. (2021). Cyber Hygiene: Daily Practices for Maintaining Cybersecurity Nagaraju Pureti. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 35-52.

[55]. Pureti, N. (2021). Incident Response Planning: Preparing for the Worst in Cybersecurity. *Revista de Inteligencia Artificial en Medicina*, *12*(1), 32-50.

[56]. Pureti, N. (2021). Penetration Testing: How Ethical Hackers Find Security Weaknesses. *InternationalJournal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *12*(1), 19-38.

[57]. Pureti, N. (2022). Building a Robust Cyber Defense Strategy for Your Business. *Revista de Inteligencia Artificial en Medicina*, *13*(1), 35-51.

[58]. Pureti, N. (2022). The Art of Social Engineering: How Hackers Manipulate Human Behavior. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *13*(1), 19-34.

[59]. Pureti, N. (2022). Zero-Day Exploits: Understanding the Most Dangerous Cyber

Threats. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(2), 70-97.

[60]. Pureti, N. (2023). Anatomy of a Cyber Attack: How Hackers Infiltrate Systems. *Revista deInteligencia Artificial en Medicina*, *14*(1), 22-53.

[61]. Pureti, N. (2023). Encryption 101: How to Safeguard Your Sensitive Information. *InternationalJournal of Advanced Engineering Technologies and Innovations*, *1*(01), 242-270.

[62]. Pureti, N. (2023). Responding to Data Breaches: Steps to Take When Your Data is Compromised. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), 27-50.

[63]. Pureti, N. (2023). Strengthening Authentication: Best Practices for Secure Logins. *InternationalJournal of Advanced Engineering Technologies and Innovations*, *1*(01), 271-293.

[64]. Pureti, N. (2024). The Rising Tide of Malware: Protecting Your Organization in 2024. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(3), 420-448.

[65]. Msekelwa, P. Z. (2024). The Impact of AI on Education: Innovative Tools and Trends. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *5*(1), 227-236.