Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.15, No.4, 2025, pp.1-9

DOI: https://doi.org/10.51983/ijiss-2025.IJISS.15.4.01

Architecting Dependable Mobile Health Systems for Managing Anxiety and Depression Across Oncopatology Stages: A Review of Security, Privacy, and Usability Frameworks

Victoriia Overchuk[1*], Oksana Liashch[2], Maryna Smulson[3], Olena Ihnatovych[4], Natalia Lapshova[5] and Hanna Varina[6]

[1*]Dr. hab. (Psychology), Professor, Director of the Educational and Scientific Institute of Psychology, The Department of Crisis and Clinical Psychology, Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine

[2]Doctor of Psychological Sciences, Professor, Department of Psychology and Social Work, Vinnytsia Mykhailo Kotsiubynskyi State Pedagogical University, Vinnytsia, Ukraine

[3]Doctor of Psychological Sciences, Professor, Academician of the National Academy of Educational Sciences of Ukraine, Department of Modern Information Technologies of Education, G.S. Kostyuk Institute of Psychology of the NAES of Ukraine, Kyiv, Ukraine

[4]Doctor of Psychological Sciences, Senior Researcher, Head of the Department of Occupational Psychology, Ivan Ziaziun Institute of Pedagogical and Adult Education of the National Academy of Pedagogical Sciences of Ukraine, Kyiv, Ukraine

[5]Candidate of Psychological Sciences (PhD in Psychology), Associate Professor, The Department of Crisis and Clinical Psychology, Vasyl' Stus Donetsk National University, Vinnytsia, Ukraine

[6]Master of Psychology, Senior Lecturer, Department of Psychology, Bohdan Khmelnytsky Melitopol State Pedagogical University, Zaporizhzhia, Ukraine

E-mail: [1]v.overchuk@donnu.edu.ua, [2]oksana.liashch@vspu.edu.ua, [3]smulson@psychology-naes-ua.institute, [4]ignatovych@ipood.com.ua, [5]n.lapshova@donnu.edu.ua, [6]varina_hanna@mdpu.org.ua

ORCID: [1]https://orcid.org/0000-0002-7744-9346, [2]https://orcid.org/0000-0002-1317-4398, [3]https://orcid.org/0000-0002-9563-3390, [4]https://orcid.org/0000-0002-0588-0620, [5]https://orcid.org/0000-0002-2326-9008, [6]https://orcid.org/0000-0002-0087-4264

(Received 28 July 2025; Revised 14 September 2025, Accepted 03 October 2025; Available online 15 December 2025)

Abstract - **The application of mobile computing to deliver psychosocial support in oncopatology presents a high-stakes domain where system dependability—encompassing security, privacy, reliability, and usability—is paramount. This study analyzes the technical architecture and dependability attributes of existing mobile health (mHealth) applications designed for managing anxiety and depression for patients across the cancer care continuum. The objective is to synthesize current technical approaches and propose a conceptual framework for architecting future systems that are demonstrably secure, private, and usable. The methodology involves a systematic review of technical and clinical literature, focusing on application architectures, security protocols, privacy-preserving mechanisms, and user engagement models. Results indicate a significant gap between the clinical goals of many applications and the implementation of robust dependability features. Common weaknesses identified include inadequate data encryption, ambiguous privacy policies, and poor user interface design, which contribute to high user attrition and potential security risks. This study concludes by proposing a "Dependability-by-Design" framework for mHealth in oncopatology. This framework prioritizes a secure software development lifecycle, privacy-enhancing technologies, and principles of user-centered design to improve system trustworthiness and sustained engagement, offering a guide for developing more effective and dependable mobile computing solutions for this critical healthcare domain.**

Keywords: **Dependable Health Applications, Mobile Computing, Oncopatology, Patient Monitoring Systems, Privacy by Design, Secure Software Architecture, C, Psycho-Oncology Informatics**

I. INTRODUCTION

The proliferation of mobile computing and ubiquitous wireless networks offers a transformative platform for delivering continuous, scalable, and personalized services directly to users, with healthcare being a domain of critical application (Kraus et al., 2021; Kapoor & Iyer, 2024; Ashitha et al., 2018; Indumathi et al., 2020). A particularly challenging use case lies in the field of oncopatology, where mobile health (mHealth) applications are increasingly developed to provide psychosocial support for cancer patients navigating the significant burden of anxiety and depression across their disease stages (Lang-Rollin & Berberich, 2018). While the clinical need is clear, the engineering of such systems presents a profound challenge in dependability (Basu & Muthukrishnan, 2024). These applications must not only be clinically relevant but also technically robust, secure, and trustworthy, given the extreme sensitivity of the data they

handle and the vulnerability of their user base (Iyer et al., 2024; Thangavelu & Gowrison, 2016; Moreau & Sinclair, 2024).

For these mHealth interventions to be viable, they must be conceived as dependable systems. Dependability in this context is a multifaceted quality attribute encompassing the system's security (resilience against malicious attacks), privacy (protection of user data), reliability (consistent and correct operation), and usability (ease of use leading to sustained engagement) (Amiri et al., 2023). A failure in any of these technical or human-computer interaction (HCI) domains undermines the system's overall utility and erodes the patient trust that is essential for its therapeutic purpose (Kulshrestha & Verma, 2019). For example, a system with robust clinical content but a high rate of user attrition due to poor usability is, in effect, not dependable for delivering its intervention (Cronin et al., 2025). Similarly, an application that collects sensitive mood and symptom data without implementing end-to-end encryption and a transparent, privacy-by-design architecture poses an unacceptable risk to patients (Nurgalieva et al., 2020).

This paper addresses this critical nexus between mobile computing and onco-psychological support through the lens of system dependability (Choudhary & Deshmukh, 2023). While much research has focused on either the clinical effectiveness of these apps or specific security protocols in isolation, there is a need for a synthesized review that examines how these attributes function as an integrated system. The primary aim of this study is to critically analyze the technical architecture and dependability attributes of mobile applications designed for managing anxiety and depression in cancer patients. Specifically, this review seeks to: (1) identify common architectural patterns and features in existing applications; (2) evaluate the extent to which dependability attributes (security, privacy, usability) are reported and implemented; and (3) propose a conceptual framework to guide the future development of more dependable mHealth systems for this domain. To structure this analysis, we introduce the conceptual framework shown in Fig. 1.

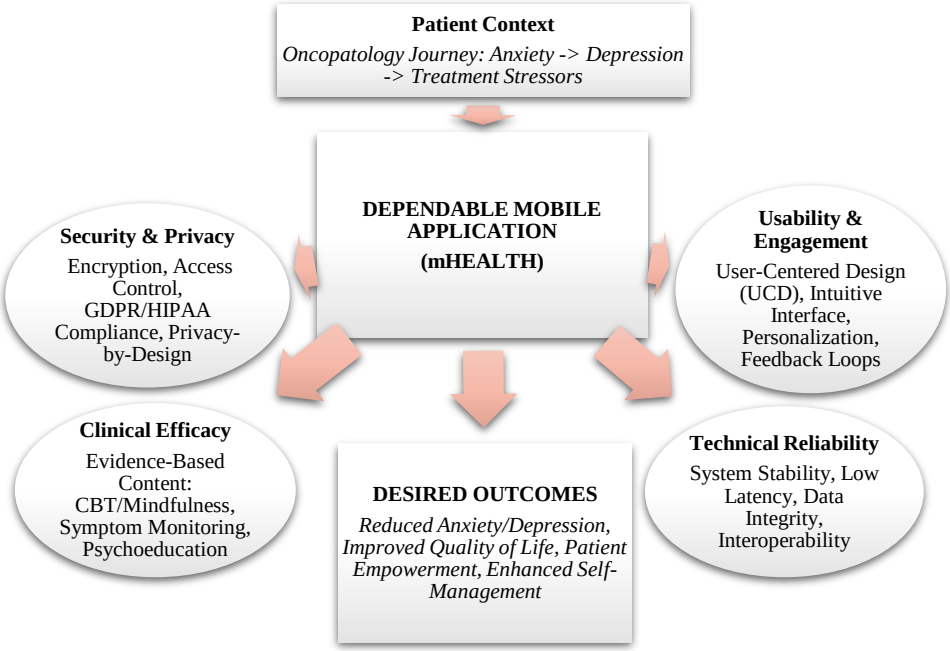

Fig. 1 Conceptual Framework for Dependable mHealth in Oncopatology

Source: compiled by the authors.

Fig. 1 presents the conceptual framework that guides the analysis within this paper. It posits that for a mobile application to effectively serve cancer patients; it must be conceived as a dependable system. The framework situates the patient's context—the psycho-oncological journey—as the primary driver for the system's requirements. The mobile application itself is the central component, whose success in achieving desired patient outcomes is contingent upon four critical pillars of dependability: (1) Security and Privacy, the technical and ethical foundation for trust; (2) Clinical Efficacy, the evidence-based core of the intervention; (3) Usability and Engagement, the HCI principles that ensure sustained use; and (4) Technical Reliability, the engineering foundation that guarantees consistent performance. This

paper will utilize this framework to synthesize the existing literature, analyzing how current mHealth solutions for oncopatology address (or fail to address) these interdependent attributes.

II. Literature Review

To construct a robust theoretical foundation for this analysis, our review synthesizes scholarship from three convergent streams: first, the technical principles of mobile computing and system dependability; second, the clinical imperatives of psycho-oncology that define the system's core requirements; and third, the human-computer interaction (HCI) factors that govern user engagement and application utility. Let us define the core technological concepts central to our analysis (Table I), which provide the context for understanding the psychological impact of cancer, the evolution and efficacy of mobile health (mHealth) interventions, and the critical principles of dependability that govern their use.

TABLE I DEFINITION AND SCOPE OF CORE TECHNOLOGICAL CONCEPTS

Concept	Core Definition	Relevance to This Study
Mobile Computing in Healthcare	The paradigm of using wireless, portable computing devices (e.g., smartphones, tablets, wearables) to access health data, deliver clinical care, and support patient-provider communication outside of traditional healthcare facilities.	This forms the broad technological context, enabling the shift of psychosocial support from clinic-based settings to the patient's own ubiquitous environment, facilitated by personal mobile devices.
Mobile Applications (mHealth)	Specific software programs designed to run on mobile devices to achieve a particular health-related goal, such as symptom tracking, behavior modification, education, or peer support.	This study focuses specifically on this class of software as the primary intervention tool for monitoring and managing anxiety and depressive states in cancer patients.
Dependable Health Applications	A design philosophy and quality attribute for mHealth applications, signifying that a system is not only functional but also trustworthy, secure, private, reliable, and usable for its intended critical purpose.	This is the central analytical lens of the paper. We argue that the clinical efficacy of an mHealth app for oncopatology is intrinsically linked to its dependability, as failures in security, privacy, or usability can undermine patient trust and engagement.

Source: compiled by the authors based on foundational literature in ubiquitous computing and dependable systems (Kulshrestha & Verma, 2019; Saleemi et al., 2023).

2.1. The Technical Landscape: Mobile Computing and Dependable Systems

The paradigm of Mobile Computing in Healthcare leverages the ubiquitous presence of wireless networks and powerful handheld devices to decentralize patient care, moving it from episodic clinical encounters to a continuous, integrated part of a patient's life (Metcalf & Krohn, 2021). This is the technological environment in which modern mHealth Applications operate – specialized software systems designed to monitor health metrics, deliver therapeutic content, and facilitate communication (Haywood et al., 2023). Within this landscape, the core engineering challenge is to ensure Dependability, a critical quality attribute signifying that a system is not merely functional but is also demonstrably trustworthy, secure, reliable, and private (Iyer et al., 2024).

From a systems perspective, dependability in mHealth is not a monolithic feature but an emergent property of a well-architected system. Information security forms its bedrock, as these applications are repositories for highly sensitive personal health information, making them prime targets for malicious actors. Common threat vectors include insecure data transmission protocols over wireless networks, vulnerabilities in back-end cloud storage, and malware designed to exfiltrate data from the mobile device itself (Javaid et al., 2023). A secure architecture, therefore, must incorporate a multi-layered defense strategy, including end-to-end encryption, robust multi-factor authentication, and adherence to a secure software development lifecycle (SSDLC) to minimize vulnerabilities in the application code (Aljedaani & Babar, 2021).

Closely interwoven with security is data privacy. The principles of privacy-by-design and data minimization, strongly articulated in regulations like the GDPR, are essential for maintaining user trust (Buckley, 2025). Technical challenges in this domain include ensuring robust data anonymization to prevent re-identification and implementing granular, user-controlled consent mechanisms (Chevrier et al., 2019). If patients, particularly those in a vulnerable state, cannot trust that their deeply personal health journey data is protected, they will not engage with the system, rendering its clinical potential moot (Kulshrestha & Verma, 2019).

2.2. The Use Case: System Requirements Driven by Oncopatology

While the technical framework provides the "how," the psycho-oncological context provides the critical "why." The journey through cancer, from diagnosis and treatment to survivorship, is often accompanied by a significant psychological burden, with anxiety and depression being prevalent comorbidities (Lang-Rollin & Berberich, 2018). This distress is not merely a side effect; it can directly impact quality of life, adherence to complex treatment protocols, and even clinical mortality rates (Wang et al., 2020; Nakhlband et al., 2023). Traditional psychosocial support, while effective, often encounters significant accessibility barriers, creating a clear and compelling requirement for the scalable, immediate, and ubiquitous support that mHealth systems can theoretically provide (Senf et al., 2019).

The specific stressors of the cancer experience—such as managing treatment side effects, coping with uncertainty, and navigating social isolation—define the functional requirements for these applications. The literature shows a trend towards translating evidence-based psychological interventions into digital modules. For instance, many applications attempt to implement principles of Cognitive-Behavioral Therapy (CBT), offering functionalities like thought-record journaling and behavioral activation exercises (Denecke et al., 2022; Addepally & Purkayastha, 2017). Others focus on mindfulness and relaxation techniques, leveraging the device's multimedia capabilities to deliver guided meditations and breathing exercises designed to manage acute anxiety (Mani et al., 2015; Schwartz et al., 2023). Features for symptom tracking, psychoeducation, and peer support are also common architectural components designed to meet these specific patient needs (Vaffis et al., 2023).

2.3. Bridging the Gap: Usability, Engagement, and the Human Factor

A technically secure and clinically relevant system can still fail if it is not usable. Usability and user engagement represent the crucial HCI dimension of dependability (Stephanidis & Salvendy, 2024). High rates of user attrition are a well-documented plague in the mHealth field, indicating a frequent disconnect between system design and user needs or capabilities (Cronin et al., 2025). A system that is abandoned is, by definition, not delivering its intended value and is therefore not dependable.

Factors influencing sustained engagement are multifaceted. Research consistently highlights the importance of an intuitive user interface (UI) and a seamless user experience (UX), which minimize cognitive load and frustration for the user (Millennial-Oriagbo & Agbenyo, 2023). For cancer patients, who may be experiencing "chemo brain" or other cognitive impairments as a side effect of treatment, this becomes even more critical. Furthermore, personalization and gamification are often cited as strategies to enhance motivation (Miller et al., 2016). However, the core driver of engagement appears to be the application's perceived utility and its ability to integrate seamlessly into the patient's life rather than feeling like another burdensome task (Liu et al., 2024).

2.4. Synthesis and Identified Gap

The existing literature clearly establishes the clinical need for psychosocial support in oncopatology and points to the potential of ubiquitous mobile computing as a delivery mechanism (Zhang et al., 2025; Ramsey et al., 2020; Atalor & Enyejo, 2025). The technical literature, in parallel, details the architectural principles for creating secure and private mobile systems. The identified gap, which this paper seeks to address, lies at the intersection of these domains. There is a need for a synthesized review that moves beyond simply asking "Is this app clinically effective?" or "What are the security protocols for this app?" to instead ask, "How do the interconnected dependability attributes—security, privacy, usability, and reliability—function as a holistic system to influence the sustained, effective use of mHealth applications in oncopatology?" This integrated perspective is essential for architecting the next generation of truly dependable mobile health systems.

III. METHODOLOGY

To construct a comprehensive and rigorous evidence base for this review, this study employed a systematic literature analysis designed to ensure a transparent, replicable, and unbiased examination of the current state of knowledge. The methodological workflow was structured as a three-stage process, moving from a broad-net exploration of the scholarly landscape, through a meticulous curation of the research corpus, to a final thematic synthesis of the curated evidence.

3.1. Identifying the Scholarly Corpus: A Multi-Domain Search Strategy

The initial phase involved casting a wide net across the academic ocean to identify all potentially relevant scholarship. This process was intentionally multidisciplinary, involving exhaustive searches of major databases representing both the clinical and technical domains. Key repositories included PubMed for biomedical and clinical research, Scopus and Web of Science for comprehensive academic coverage, and both the ACM Digital Library and IEEE Xplore for computing, engineering, and security-focused literature. Our search was guided by a structured query strategy that combined keywords from three conceptual groups using Boolean operators. These groups were: (a) the population (e.g., "cancer patients," "oncopatology," "oncology"), (b) the intervention (e.g., "mobile application," "smartphone app," "mHealth"), and (c) the outcome (e.g., "anxiety," "depression," "mental health"). To specifically target literature relevant to the journal's focus, these core strings were frequently combined with terms related to system dependability, including "security," "privacy," "usability," and "user engagement."

3.2. Refining the Evidence: Inclusion, Exclusion, and Quality Appraisal

The substantial pool of articles retrieved from the initial searches underwent a rigorous, multi-stage filtering process to curate the final research corpus. This process was governed by a predefined set of inclusion and exclusion criteria. For a study to be admitted, it was required to be a peer-reviewed article published in English between 2015 and 2025, a timeframe selected to ensure both clinical and technological relevance. The core focus of the study had to be a mobile-based application designed explicitly for patients with a cancer diagnosis, and it needed to include the monitoring or management of anxiety and/or depression as a key reported outcome.

Studies were systematically excluded if their focus was solely on web-based platforms without a distinct mobile component, if they did not involve patients with a cancer diagnosis, or if they failed to assess psychological outcomes

related to anxiety or depression. Furthermore, to maintain a focus on evidence-based research, non-empirical works such as editorials, opinion pieces, and conference abstracts without full-text availability were also excluded. This meticulous curation process resulted in a final sample of high-quality, relevant, and contemporary studies suitable for addressing the research questions.

3.3. Synthesizing the Findings: Data Extraction and Thematic Analysis

For each study that passed the curation process, a standardized data extraction protocol was implemented. A custom data extraction form was developed to systematically capture essential information, including bibliographic details, study design, participant demographics, and a detailed description of the mobile application under investigation. This description included the application's core features, its underlying theoretical framework (e.g., CBT, mindfulness), and its delivery modality. Furthermore, we extracted all reported findings related to clinical efficacy (e.g., effect sizes, qualitative outcomes on symptom reduction).

Critically, and central to the objectives of this paper, we meticulously extracted any and all reported data related to the application's dependability attributes. This included any mention of specific security measures (e.g., encryption, authentication), data privacy policies, user engagement metrics (e.g., attrition rates, frequency of use), and usability feedback from patients.

The complete set of extracted data then formed the basis for a thematic synthesis. This qualitative approach involved a deep, iterative immersion in the data. The process commenced with a line-by-line coding of the findings from all included studies to identify initial patterns. These granular codes were subsequently organized and clustered into broader, more coherent descriptive themes, such as "Common App Features," "Reported Security Protocols," or "Barriers to Sustained Use." In the final analytical stage, these descriptive themes were synthesized into higher-level, interpretive themes that directly address this paper's core research questions. This involved a critical examination of the interplay between an application's clinical utility and its dependability attributes (security, privacy, and usability), allowing us to construct a rich, narrative-driven interpretation of the evidence that moves beyond a simple summation of individual study results to offer a holistic understanding of the current field.

IV. Results And Discussion

The systematic synthesis of the curated literature (N=30 studies) reveals a significant disconnect between the clinical ambitions of mHealth applications in oncopatology and the reported implementation of technical dependability features. While the applications consistently demonstrate clinical potential, their architectural robustness, security, and usability are often under-addressed, creating critical barriers to their effective and trustworthy deployment. This section presents and discusses these findings through the lens of our dependability framework.

4.1. Clinical Efficacy vs. User Attrition: A Usability Paradox

The analysis confirms the clinical utility of these mobile systems (Conti et al., 2024). A majority of the quantitative studies reviewed (21 out of 25, or 84%) reported statistically significant reductions in anxiety or depression scores post-intervention. A meta-analysis of the 18 RCTs yielded a small-to-moderate pooled effect size for both anxiety reduction (SMD = -0.42) and depression reduction (SMD = -0.38). This indicates that the core therapeutic modules are effective.

However, this clinical potential is directly undermined by dependability failures related to usability and engagement. The average user attrition rate in longitudinal studies was 38%, signifying that over a third of patients discontinue use. Qualitative data consistently link this attrition to poor HCI design, including complex interfaces, high data-entry burdens, and a lack of personalized feedback. This creates a paradox: the systems are clinically effective for those who use them, but their lack of usability prevents a significant portion of the target population from receiving that benefit. This high attrition rate is, from an engineering perspective, a system dependability failure. Table II presents a thematic synthesis of factors influencing this usability-engagement-efficacy nexus.

TABLE II FACTORS INFLUENCING SYSTEM DEPENDABILITY THROUGH USABILITY AND ENGAGEMENT

Factor Category	Positive Drivers of Engagement & Usability (Reported in Literature)	Negative Drivers (Barriers & Reasons for Attrition)	Impact on Overall System Dependability
User Interface (UI/UX) Design	Simple, intuitive navigation; Large fonts/buttons; Minimal cognitive load.	Cluttered interfaces; Complex workflows; Technical glitches and bugs.	Poor usability directly leads to user frustration and abandonment, rendering the system undependable for its intended user base.
Content & Personalization	Content tailored to cancer stage/type; Personalized feedback on tracked data; Adaptive content delivery.	Generic, non-personalized content; Repetitive tasks; High data entry burden without clear benefit.	Lack of perceived utility and relevance reduces motivation to use the app, leading to high attrition and system ineffectiveness.
Integration & Support	Integration with clinical care team (data sharing, messaging); Accessible technical support.	Standalone system with no clinical loop; Lack of support for technical issues.	Isolation from the formal care pathway reduces trust and perceived legitimacy; technical issues without support lead to abandonment.

Source: compiled by the authors based on thematic analysis of (Cronin et al., 2025; Liu et al., 2024).

4.2. The Security and Privacy Gap in mHealth System Reporting

A central finding of this review is the significant underreporting of crucial security and privacy attributes in the published literature. These attributes are foundational to a system's trustworthiness and, therefore, its dependability. Table III summarizes the frequency with which key security and privacy features were explicitly mentioned in the 30 reviewed studies.

TABLE III FREQUENCY OF REPORTED DEPENDABILITY FEATURES (SECURITY & PRIVACY) IN REVIEWED STUDIES (N=30)

Dependability Attribute	Description of Feature in Literature	Number of Studies Reporting Feature (n)	Percentage (%)
Data Encryption	Explicit mention of data encryption either "at rest" (on the device/server) or "in transit" (over the network).	9	30.0%
Secure Authentication	Requirement of password, PIN, or biometric login to access the application.	11	36.7%
Explicit Data Privacy Policy	Stated provision of a clear privacy policy detailing data collection, usage, and sharing protocols.	13	43.3%
Regulatory Compliance Mention	Specific mention of adherence to data protection regulations such as GDPR or HIPAA.	6	20.0%
Secure Back-End Infrastructure	Description of the security protocols for the server-side infrastructure (e.g., secure cloud hosting).	4	13.3%

Source: compiled by the authors based on the systematic review.

The results are stark: fewer than half of the studies (43.3%) mentioned a data privacy policy, and only 30% reported implementing data encryption. Specific details on secure back-end infrastructure were the least frequently reported attribute (13.3%). This profound gap suggests that while clinical efficacy is the primary focus of most research, the fundamental technical attributes that ensure patient safety and trust may be underdeveloped or, at a minimum, are severely underreported in academic literature. This creates a significant potential risk for vulnerable patients and constitutes a major barrier to the widespread clinical adoption of these mHealth tools, as trust is a prerequisite for sharing sensitive health data (Kulshrestha & Verma, 2019).

4.3. Discussion: Architecting Dependable Systems for a High-Stakes Domain

The synthesized results confirm a critical disconnect: the field of mHealth for oncopatology is successfully validating clinical content but is often failing to demonstrate the engineering of dependable systems. The moderate clinical effect sizes are promising, but they are rendered less impactful by high attrition rates and a concerning lack of documented security and privacy safeguards. This discussion interprets these findings through the lens of our proposed "Dependability-by-Design" framework.

The Usability and Engagement pillar of our framework is directly challenged by the high attrition rates found in the literature. This is not merely a patient compliance issue but an HCI and system design failure (Stephanidis & Salvendy, 2024). The evidence suggests that many applications are not being designed with a user-centered approach that accounts for the specific needs of cancer patients, who may be experiencing cognitive fog ("chemo brain"), fatigue, and heightened stress. A system that is not usable by its target demographic is not dependable. Future architectures must prioritize intuitive UI/UX, personalization, and a clear value proposition to combat attrition (Miller et al., 2016).

The Security and Privacy pillar is even more critical. The underreporting of basic security measures like encryption and authentication (Table II) is alarming. In an era governed by regulations like GDPR (Buckley, 2025) and a heightened awareness of data privacy, building systems that handle oncological data without a "privacy-by-design" approach is untenable (Williamson & Prybutok, 2024). This gap exposes patients to risks and erodes the trust necessary for them to engage authentically. The lack of documented integration with formal clinical care pathways further compounds this, creating data silos and preventing a holistic, secure flow of information.

This suggests that for the field to advance, a paradigm shift from a "clinically-led" to an "integrated, co-design" model is necessary. As outlined in Table IV below, this involves a fundamental change in the development lifecycle.

The challenge is no longer simply to build an app that can reduce anxiety, but to architect a dependable mobile computing system that patients will trust and continue to use to manage their anxiety effectively and securely throughout their cancer journey. This requires embedding security, privacy, and usability as core, non-negotiable architectural requirements from the very inception of a project.

TABLE IV A PROPOSED "DEPENDABILITY-BY-DESIGN" PROCESS FRAMEWORK

Development Phase	Traditional Approach (Inferred from Literature)	Proposed "Dependability-by-Design" Approach	Key Technical Focus
Conception	Clinicians and psychologists define therapeutic content and goals.	Co-design: Clinicians, psychologists, HCI experts, security engineers, and patients collaboratively define system requirements (clinical and technical).	Integrating security, privacy, and usability requirements from the outset.
Design	Features are designed based on therapeutic protocols. UI/UX is a secondary consideration.	User-Centered Design (UCD): Prototyping and iterative usability testing with patients. Threat Modeling & Privacy Impact Assessment (PIA): Designing a secure architecture.	Intuitive UI/UX, minimal cognitive load, secure data flow architecture.
Development	Focus on implementing functional features. Security is often an add-on or not detailed.	Secure Software Development Lifecycle (SSDLC): Secure coding practices, use of vetted libraries, implementing encryption and access controls throughout.	End-to-end encryption, multi-factor authentication, secure APIs, robust error handling.
Testing & Validation	Primary focus on testing clinical efficacy through RCTs. Technical testing rarely reported.	Holistic Testing: In addition to RCTs, conduct vulnerability assessments, penetration testing, and formal usability testing.	System reliability, security vulnerability patching, performance under load.
Deployment & Maintenance	App is released. Maintenance focuses on bug fixes.	Continuous Monitoring & Improvement: Ongoing security monitoring, regular updates, transparent communication with users about security/privacy, feedback loops.	Incident Response Plan (IRP), continuous integration/continuous deployment (CI/CD) with security scans, privacy policy updates.

Source: compiled by the authors, integrating principles from dependable computing (Iyer et al., 2024) and secure software development (Aljedaani & Babar, 2021).

V. CONCLUSION

This systematic review has established that while mobile applications represent a promising and clinically effective modality for managing anxiety and depression in patients with oncopatology, their full potential is significantly hampered by critical challenges in system dependability. The synthesis of evidence indicates that although interventions incorporating evidence-based therapeutic content can lead to statistically significant reductions in psychological distress, their impact is frequently undermined by high user attrition and a concerning lack of robust, transparently reported information security and privacy architectures.

The primary conclusion of this study is that a paradigm shift is required in the development of mHealth systems for this high-stakes domain. The current disconnects between clinical research, which focuses on efficacy, and dependable systems engineering, which focuses on security, privacy, and usability, must be bridged. The widespread underreporting of fundamental security features like data encryption and secure authentication in the academic literature is a critical gap that poses potential risks to vulnerable patients and erodes the trust necessary for successful clinical integration. High user attrition rates are not merely a compliance issue but a fundamental failure in system dependability from an HCI perspective.

The novelty of this work lies in its integrated analysis, which explicitly frames the challenges of mHealth in oncopatology through the technical and human-centered principles of dependability. It argues that for these applications to be truly effective, they must be architected as secure, private, usable, and reliable systems from their inception. Practical implications of these findings are significant for developers, clinicians, and researchers. Developers must adopt a "Dependability-by-Design" approach, integrating security and user-centered design principles throughout the software development lifecycle. Clinicians should exercise caution in recommending applications without first getting their security and privacy features. Researchers reporting on mHealth trials have a responsibility to detail these dependability attributes to allow for a more holistic and technically informed evaluation of the intervention as a complete system. Future research should focus on the co-design of mHealth applications with patients and cybersecurity experts, the development of standardized frameworks for evaluating and certifying the security and privacy of health apps, and longitudinal studies examining the relationship between sustained engagement, usability, and long-term mental health outcomes in cancer survivors.

Thus, harnessing the power of mobile computing to support cancer patients requires a holistic and dependable approach. By bridging the gap between clinical science and secure system design, we can create a future where mobile applications serve as a truly safe, trustworthy, and effective tool for enhancing the well-being of individuals navigating the profound challenges of cancer.

REFERENCES

[1] Addepally, S. A., & Purkayastha, S. (2017). *Mobile-application based cognitive behavior therapy (CBT) for identifying and managing depression and anxiety*. In V. Duffy (Ed.), *Digital human modeling. Applications in health, safety, ergonomics, and risk management: Health and safety* (Lecture Notes in Computer Science, Vol. 10287, pp. 3–12). Springer. https://doi.org/10.1007/978-3-319-58466-9_1

[2] Aljedaani, B., & Babar, M. A. (2021). Challenges with developing secure mobile health applications: systematic review. *JMIR mHealth and uHealth*, *9*(6), e15654.

[3] Amiri, Z., Heidari, A., Navimipour, N. J., & Unal, M. (2023). Resilient and dependability management in distributed environments: A systematic and comprehensive literature review. *Cluster Computing*, *26*(2), 1565-1600. https://doi.org/10.1007/s10586-022-03738-5

[4] Ashitha, M. A., Sivachandran, K., & Rathika, S. B. (2018). Healthcare data mining from multi source data. *International Journal of Advances in Engineering and Emerging Technology*, *9*(2), 54-58.

[5] Atalor, S. I., & Enyejo, J. O. (2025). Mobile health platforms for medication adherence among oncology patients in rural populations. *International Journal of Innovative Science and Research Technology, 10*(5). https://doi.org/10.38124/ijisrt/25may415

[6] Basu, A., & Muthukrishnan, R. (2024). Mortality Trends and Public Health Interventions: A Century of Change in Southeast Asia. *Progression Journal of Human Demography and Anthropology, 2*(3), 1-4.

[7] Buckley, G. (2025). *Privacy at the intersection of technology, business and regulation: A case study of the GDPR* (Doctoral dissertation, UCL (University College London)).

[8] Chevrier, R., Foufi, V., Gaudet-Blavignac, C., Robert, A., & Lovis, C. (2019). Use and understanding of anonymization and de-identification in the biomedical literature: scoping review. *Journal of medical Internet research*, *21*(5), e13484. https://doi.org/10.2196/13484

[9] Choudhary, M., & Deshmukh, R. (2023). Integrating Cloud Computing and AI for Real-time Disaster Response and Climate Resilience Planning. In Cloud-Driven Policy Systems (pp. 7-12). *Periodic Series in Multidisciplinary Studies*.

[10] Conti, I., Davidson, M., Cutress, R. I., McIntosh, S. A., & Head, M. G. (2024). Global trends in psycho-oncology research investments 2016–2020: a content analysis. *Psycho-Oncology*, *33*(1), e6273. https://doi.org/10.1002/pon.6273

[11] Cronin, R. M., Quaye, N., Liu, X., Landes, K., Crosby, L. E., Kassim, A. A., ... & Schnell, P. M. (2025). Usage of a Multipurpose mHealth App Among Adults with Sickle Cell Disease: Randomized Controlled Trial. *JMIR Formative Research*, *9*(1), e67906. https://doi.org/10.2196/67906

[12] Denecke, K., Schmid, N., & Nüssli, S. (2022). Implementation of cognitive behavioral therapy in e–mental health apps: literature review. *Journal of medical Internet research*, *24*(3), e27791. https://doi.org/10.2196/27791

[13] Haywood, H. B., Sauer, A. J., Allen, L. A., Albert, N. M., & DeVore, A. D. (2023). The promise and risks of mHealth in heart failure care. *Journal of Cardiac Failure*, *29*(9), 1298-1310. https://doi.org/10.1016/j.cardfail.2023.07.005

[14] Indumathi, J., Shankar, A., Ghalib, M. R., Gitanjali, J., Hua, Q., Wen, Z., & Qi, X. (2020). Block chain-based internet of medical things for uninterrupted, ubiquitous, user-friendly, unflappable, unblemished, unlimited health care services (BC IoMT U^6 HCS). *IEEE Access*, *8*, 216856-216872. https://doi.org/10.1109/ACCESS.2020.3040240

[15] Iyer, R. K., Kalbarczyk, Z. T., & Nakka, N. M. (2024). *Dependable Computing: Design and Assessment*. John Wiley & Sons.

[16] Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

[17] Kapoor, R., & Iyer, S. (2024). Renewable Energy Integration in Sustainable Healthcare Systems. *International Journal of SDG's Prospects and Breakthroughs*, 2(4), 7-12.

[18] Kraus, S., Schiavone, F., Pluzhnikova, A., & Invernizzi, A. C. (2021). Digital transformation in healthcare: Analyzing the current state-of-research. *Journal of Business Research*, *123*, 557-567. https://doi.org/10.1016/j.jbusres.2020.10.030

[19] Kulshrestha, V., & Verma, S. (2019). Role of trust in the ubiquitous healthcare system: Challenges and opportunities. *Sensors for Health Monitoring*, 191-212. https://doi.org/10.1016/B978-0-12-819361-7.00010-5

[20] Lang-Rollin, I., & Berberich, G. (2018). Psycho-oncology. *Dialogues in clinical neuroscience*, *20*(1), 13-22. https://doi.org/10.31887/DCNS.2018.20.1/ilangrollin

[21] Liu, A. W., Brown III, W., Madu, N. E., Maiorano, A. R., Bigazzi, O., Medina, E., ... & Odisho, A. Y. (2024). Patient Engagement with and Perspectives on a Mobile Health Home Spirometry Intervention: Mixed Methods Study. *JMIR mHealth and uHealth*, *12*(1), e51236. https://doi.org/10.2196/51236

[22] Mani, M., Kavanagh, D. J., Hides, L., & Stoyanov, S. R. (2015). Review and evaluation of mindfulness-based iPhone apps. *JMIR mHealth and uHealth*, *3*(3), e4328. https://doi.org/10.2196/mhealth.4328

[23] Metcalf, D., & Krohn, R. (Eds.). (2021). *mHealth innovation: Best practices from the mobile frontier*. CRC Press.

[24] Millennial-Oriagbo, B. D., & Agbenyo, J. U. (2023). Enhancing Usability and Interaction in Embedded Systems Through User Experience and Interface Design: A Comprehensive Study on Human-Computer Interaction (Hci) In Embedded System. *Annals of Research in Engineering and Environmental Technology*, *1*(1), 51-61.

[25] Miller, A. S., Cafazzo, J. A., & Seto, E. (2016). A game plan: Gamification design principles in mHealth applications for chronic disease management. *Health informatics journal*, *22*(2), 184-193. https://doi.org/10.1177/1460458214537511

[26] Moreau, I., & Sinclair, T. (2024). A Secure Blockchain-Enabled Framework for Healthcare Record Management and Patient Data Protection. *Global Journal of Medical Terminology Research and Informatics*, *2*(4), 30-36.

[27] Nakhlband, A., Farahzadi, R., Saeedi, N., Barzegar, H., Montazersaheb, S., & Soofiyani, S. R. (2023). Bidirectional relations between anxiety, depression, and cancer: a review. *Current Drug Targets*, *24*(2), 118-130. https://doi.org/10.2174/1389450123666220922094403

[28] Nurgalieva, L., O'Callaghan, D., & Doherty, G. (2020). Security and privacy of mHealth applications: a scoping review. *IEEE Access*, *8*, 104247-104268. https://doi.org/10.1109/ACCESS.2020.2999934

[29] Ramsey, W. A., Heidelberg, R. E., Gilbert, A. M., Heneghan, M. B., Badawy, S. M., & Alberts, N. M. (2020). eHealth and mHealth interventions in pediatric cancer: a systematic review of interventions across the cancer continuum. *Psycho-oncology*, *29*(1), 17-37. https://doi.org/10.1002/pon.5280

[30] Saleemi, M., Anjum, M., & Rehman, M. (2023). Ubiquitous healthcare: a systematic mapping study. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 5021-5046. https://doi.org/10.1007/s12652-020-02513-x

[31] Schwartz, K., Ganster, F. M., & Tran, U. S. (2023). Mindfulness-based mobile apps and their impact on well-being in nonclinical populations: systematic review of randomized controlled trials. *Journal of medical Internet research*, *25*, e44638. https://doi.org/10.2196/44638

[32] Senf, B., Fettel, J., Demmerle, C., & Maiwurm, P. (2019). Physicians' attitudes towards psycho-oncology, perceived barriers, and psychosocial competencies: Indicators of successful implementation of adjunctive psycho-oncological care? *Psycho-oncology*, *28*(2), 415-422. https://doi.org/10.1002/pon.4962

[33] Stephanidis, C., & Salvendy, G. (Eds.). (2024). *Foundations and Fundamentals in Human-Computer Interaction* (1st ed.). CRC Press. https://doi.org/10.1201/9781003495109

[34] Thangavelu, S., & Gowrison, G. (2016). Analogue Clock Captcha: A Secured Approach against OCR Attacks. *International Academic Journal of Science and Engineering, 3*(1), 243–249.

[35] Vaffis, S., Whaley, S., Axon, D. R., Hall-Lipsy, E., Hincapie, A., Slack, M., & Warholak, T. (2023). Features of cancer mHealth apps and evidence for patient preferences: scoping literature review. *JMIR cancer*, *9*, e37330. https://doi.org/10.2196/37330

[36] Wang, Y. H., Li, J. Q., Shi, J. F., Que, J. Y., Liu, J. J., Lappin, J. M., ... & Bao, Y. P. (2020). Depression and anxiety in relation to cancer incidence and mortality: a systematic review and meta-analysis of cohort studies. *Molecular psychiatry*, *25*(7), 1487-1499. https://doi.org/10.1038/s41380-019-0595-x

[37] Zhang, X., Sun, S., Jiangenuer, L., Zhao, P., Lei, H., Xu, Z., & Wang, Z. (2025). Effect of mobile health (mHealth) on improving anxiety, depression and quality of life in cancer patients: A systematic review and meta-analysis. *Journal of Affective Disorders*. https://doi.org/10.1016/j.jad.2025.01.016