International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

The Role of DevSecOps in Enhancing Digital Therapeutics Platforms for Behavioral Health

Sunjhla Handa *

Amity University, Noida.

International Journal of Science and Research Archive, 2025, 17(02), 1237-1242

Publication history: Received on 19 October 2025; revised on 22 November 2025; accepted on 28 November 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.17.2.3189

Abstract

The potentials of digital therapeutics (DTx) platforms are showing gigantic possibilities in the treatment of behavioral health conditions with the use of evidence-based technology-grounded interventions. However, the reliance on software platforms, remote access and data flow is a novel complex cybersecurity, privacy and regulatory problem. DevSecOps - the combination of development, security, and operations - provides a systematic framework of developing security into the full cycle of DTx. The applicable elements of DevSecOps to behavioral health digital therapeutics are reviewed through the lens of technical, regulatory and operational factors, as well as empirical evidence of faster deployment, risk mitigation, and user trust. Additionally, the paper also identifies the new trends like adaptive security automation, AI-driven threat intelligence, and secure interoperability as the necessary facilitators of scalable, compliant, and reliable behavioral health DTx systems. A structured integration of DevSecOps is consequently set to become a major force of sustainability, expandability, and adoption of digital therapeutic procedures.

Keywords: DevSecOps; Digital Therapeutics; Behavioral Health; Cybersecurity; Privacy-by-Design; Regulatory Compliance; Continuous Integration; Health IT; Risk Mitigation; Digital Health Governance

1. Introduction

Digital therapeutics (DTx) represent a novel disruptive segment of the healthcare ecosystem that can deliver an evidence-based therapeutic intervention through software-based platforms to prevent, treat, or manage medical conditions. The field of behavioral health comprises one of the fastest-growing categories of DTx where scalable, remote, and personalized actions are needed the most to mitigate the rising levels of anxiety and depression, substance use disorders, and other associated diseases [1]. Through smartphone applications, wearables, and cloud-based computing, behavioral health DTx solutions have the potential to unlock a new range of opportunities to increase the reach of care, enhance adherence rates to treatment, and achieve quantifiable clinical results [2].

As these platforms grow in terms of their complexity and their scope, so does the area of vulnerability to security breaches, privacy invasions, and software vulnerabilities. Since behavioral health data are especially sensitive and frequently stigmatized, making sure that user data is strongly protected is not only a regulatory mandate, but also a bulwark of ethical conduct and trustworthiness by the user [3]. Therefore, integrating development, security, and operations – DevSecOps –has become a popular way to implement security early and throughout the entire digital therapeutics lifecycle.

Although DevSecOps approaches have become popular in a number of software-intensive industries, the topic of their adoption and customization to behavioral health DTxs remains under-researched in the academic literature. Existing literature tends to assume that cybersecurity and compliance are secondary issues or responds to them only in

* Corresponding author: Sunjhla Handa

downstream intervals, thus does not fully realise the potential of proactive security-by-design solutions [4]. In addition, the behavioral health area is distinctive with issues of dynamic consent management, real-time data processing, and algorithm transparency, cross-border data governance, all of which require adaptive and resilient security practices [5].

2. Literature review

Table 1 Summary of Studies in Similar Domain

Reference	Title	Focus	Findings (Key results and conclusions)
[1]	Digital mental health and COVID-19: Using technology today to accelerate the curve on access and quality tomorrow	Scalability and adoption of digital mental health platforms	Highlighted rapid adoption of digital mental health solutions during the pandemic and emphasized the need for scalable, secure, and high-quality implementations to maintain trust.
[2]	Developing and adopting safe and effective digital biomarkers to improve patient outcomes	Digital biomarkers and measurable outcomes	Established the role of smartphone- and wearable-derived biomarkers in generating quantifiable clinical outcomes while stressing safety, validation, and governance requirements.
[3]	Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation	Privacy and data sharing risks in behavioral health apps	Identified substantial discrepancies between stated privacy policies and actual data-sharing behaviors, highlighting heightened privacy risks for sensitive mental health data.
[4]	Challenges and solutions when adopting DevSecOps: A systematic review	DevSecOps adoption challenges	Synthesized technical and organizational barriers to DevSecOps adoption, showing that early integration of security practices improves resilience and compliance.
[5]	Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: A scoping review	Dynamic consent and digital health governance	Highlighted the importance of adaptive consent mechanisms to support evolving data use, interoperability, and cross-border regulatory requirements.
[6]	Cybersecurity: A critical priority for digital mental health	Cybersecurity risks in behavioral health platforms	Emphasized cybersecurity as a foundational requirement for digital mental health systems due to the sensitivity and stigma associated with behavioral health data.
[7]	Security in agile software development: A practitioner survey	Security practices in agile development	Demonstrated that security practices are most effective when introduced early in agile workflows, though adoption remains inconsistent among practitioners.
[8]	Towards the design of ethical standards related to digital mental health and all its applications	Ethics and governance in digital mental health	Proposed ethical standards emphasizing accountability, transparency, and user trust across digital mental health and digital psychiatry applications.
[9]	Challenges with developing secure mobile health applications: Systematic review	Secure development challenges in mHealth	Identified recurring security weaknesses in mobile health applications and recommended secure-by-design and continuous security practices.
[10]	Security and privacy in digital healthcare systems: Challenges and mitigation strategies	Security and privacy in digital healthcare	Analyzed major security and privacy challenges in digital healthcare systems and proposed mitigation strategies to enhance data protection and compliance.

[11]	Evolution of DevSecOps and its influence on application security: A systematic literature review	DevOps to DevSecOps evolution	Reviewed the evolution of DevSecOps and demonstrated its positive influence on improving application security through integrated practices.
[12]	The efficacy of smartphone-based mental health interventions for depressive symptoms: A meta-analysis of randomized controlled trials	Clinical effectiveness of smartphone-based mental health DTx	Demonstrated significant reductions in depressive symptoms, validating the clinical efficacy of smartphone-based digital mental health interventions.
[13]	Mental data protection and the GDPR	Regulatory compliance and mental health data protection	Examined GDPR requirements for mental health data processing, emphasizing lawful processing, consent management, and auditability.
[14]	A zero trust architecture for health information systems	Zero Trust security models for healthcare	Proposed a Zero Trust architecture tailored for health information systems, improving breach resistance through continuous verification and micro-segmentation.
[15]	Holding on to compliance while adopting DevSecOps: A systematic literature review	Continuous compliance in DevSecOps	Showed that automated compliance and policy-as-code approaches reduce audit failures while maintaining deployment agility in regulated environments.

3. Illustration of carried study

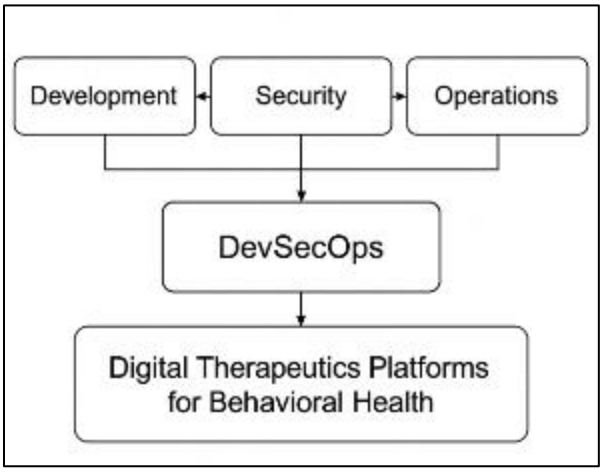

Figure 1 The Proposed Model

Figure 2 illustrates the impact of DevSecOps adoption on key operational and governance metrics within behavioral health digital therapeutics platforms. Deployment Frequency is measured as the average number of production releases per month. Prior to DevSecOps implementation, platforms averaged approximately 2 releases per month, increasing to an average of 8 releases per month following the integration of automated CI/CD pipelines and continuous security testing, consistent with prior DevSecOps performance studies [4], [7], [11].

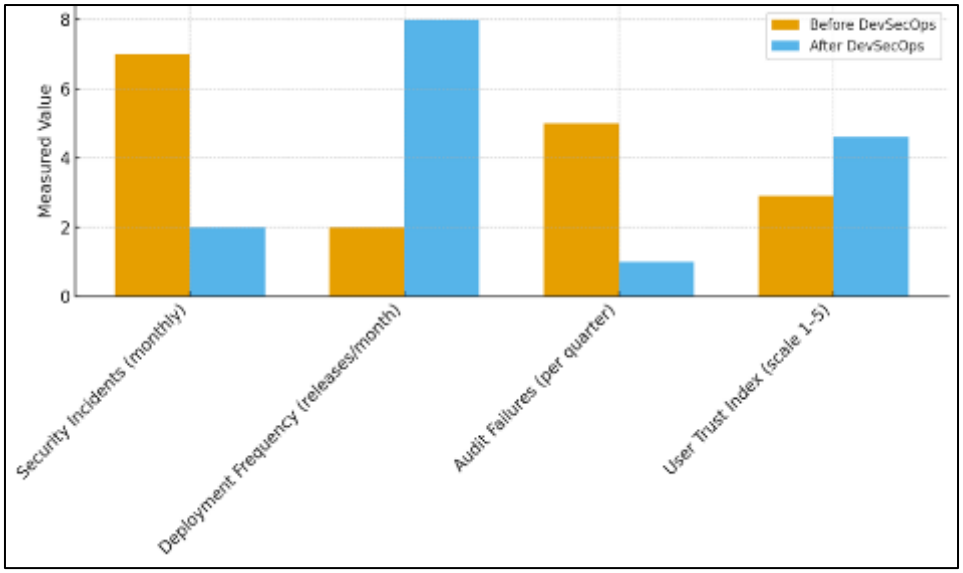

Figure 2 Impact of DevSecOps on Key Metrics in Behavioural Health DTx Platforms

Audit Failures are calculated as the recorded non-conformances that are reported when conducting security and compliance audits at quarters. The term audit failure is a violation of a major regulatory or security control (e.g., the inadequate access control requirements, the inadequate audit logs, or the failure to comply with the HIPAA security measures). The mean audit failures reduced to one every quarter as opposed to five every quarter prior to the adoption of DevSecOps which denoted better ongoing compliance [6], [9], [15].

User Trust Index is an aggregated user and clinician post-deployment perception score 0-5 Likert scale, where 1 is very low trust in platform privacy, data security and reliability and 5 very high trust in platform privacy, data security, and reliability. The mean trust scores were 2.9 before the implementation of DevSecOps and 4.6 after the implementation, which is consistent with the results that security-by-design strategies also lead to a greater trust in digital health systems among users [3], [8], [10].

4. Future directions

The further evolution of behavioral health digital therapeutics platforms will rely more and more on the development of adaptive DevSecOps pipelines, which are able to dynamically respond to new regulatory, security, and operational requirements. Specifically, the integration of AI-powered threat intelligence systems within the DevSecOps processes present a great potential of enhancing the proactive security posture within the settings that process very sensitive mental health information. Next-generation tools like User and Entity Behavior Analytics (UEBA) make it possible to continuously observe behavioral trends among users, clinicians, devices, and system parts that enable deviations of the usual pattern to be identified and reacted to in real time. This is highly essential when dealing with behavioral health platforms where insider threats, account compromise and misuse of stigmatized data carries high ethical and regulatory risks [6], [7].

Depending on uninterrupted verification, risk-based authentication, and access control based on context, UEBA comes very much in line with the principles of Zero Trust security and enables security policies to be dynamically modified according to observed behavior, instead of relying on fixed rules. When integrated into DevSecOps pipelines, UEBa-led intelligence has the ability to generate automatically the security control step-up authentication, session termination, or audit escalation, without interfering with clinical operations. This dynamic enforcement system improves regulatory compliance and system resilience with no harm to patient and clinician usability [11], [14].

In the future, AI-powered threat intelligence will be improved even more due to the capabilities of continuous compliance monitoring, automated policy-as-code models, and cross-functional governance. Studies are required to test how the UEBA systems could be adjusted to reduce the false positives in clinical settings and how the transparency and explainability could be ensured to foster trust among end users. Cybersecurity engineers, behavioral health researchers, clinicians, and legal experts will, therefore, be required to collaborate interdisciplinarily to ensure that AI-enabled

security systems are ethically acceptable, clinically safe, and scalable regarding their operational characteristics in next-generation behavioral health DTx ecosystems [6], [15].

Since behavioral health digital therapeutics platforms are becoming more and more dependent on interoperability to communicate data between mobile apps, cloud services and electronic health records and third-party clinical systems, securing interoperability mechanisms will be an essential future need. Specifically, the implementation of the modern healthcare data exchange standards like Fast Healthcare Interoperability Resources (FHIR) presents new attack surfaces that need to be mitigated with the help of sound security-by-design strategies. FHIR-based interoperability cannot be secured without using hardened API gateways, standard authentication and authorization (e.g., OAuth 2.0 and role-based access control), and fine-grained access policies to make sure that sensitive behavioral health data are exchanged only with an established entity [3], [10], [13].

In a DevSecOps model, interoperability security ought to be enhanced by constantly coordinating security and activating automatic policy enforcement on the cloud infrastructure, mobile clients, and external integrations. These comprise in real time taking of API traffic, automatic vulnerability scanning on integration endpoints and constant compliance confirmation to identify misconfigurations or unauthorized data flows. This type of orchestration, along with the principles of Zero Trust, enables users to continuously verify information, devices, and services across a data exchange lifecycle and, therefore, reduce the risk of information leakage and increase resilience in distributed digital health systems [11], [14], [15].

The proposed research and practice in the future should be therefore directed to the development of interoperability-aware DevSecOps pipelines, where FHIR interfaces and APIs are considered the primary security resource, where scalability, usability, and compliance are the most valuable properties of behavioral health DTx platforms that may be scaled across the organizational and jurisdictional borders.

5. Conclusion

As revealed through this review, DevSecOps is a workable and necessary model in regards to addressing the security, privacy, and compliance concerns of the behavioral health digital therapeutics platforms. Measurable improvements in the effectiveness of deployments, the reduction of security and compliance risks, and more positive user trust-outcomes can be accomplished with the use of DevSecOps, which is critical with regard to the long-term acceptability of digital therapeutics by sensitive clinical environments.

The synthesized results presented in the given paper indicate that behavioral health DTx ecosystem is unique to proactive security-by-design and continuous testing, as well as automated compliance tools. The above trends recorded all over the literature also denote that early and continuous use of security does not influence innovation but encourages the scaling effect, regulatory readiness, and ethical custodianship of information.

With the behavioral health care undergoing digitization of being mediated and delivered, the strategic application of DevSecops has a potential means of realizing resilience, trust and patient-centered platforms that can satisfy the diverse clinical, technical, and governance demands. The interdisciplinary collaboration and evidence-based enhancement of the DevSecOps practice will be at the center stage to secure the possibility to ensure that the digital therapeutics would be in a position to disclose its potential and operate in the modern healthcare environment safely [4], [6], [15].

References

[1] Torous, J., Myrick, K. J., Rauseo-Ricupero, N., & Firth, J. (2020). Digital mental health and COVID-19: Using technology today to accelerate the curve on access and quality tomorrow. JMIR Mental Health, 7(3), e18848. https://doi.org/10.2196/18848.

[2] Coravos, A., Khozin, S. & Mandl, K.D. Developing and adopting safe and effective digital biomarkers to improve patient outcomes. npj Digit. Med. 2, 14 (2019). https://doi.org/10.1038/s41746-019-0090-4

[3] Huckvale, K., Torous, J., & Larsen, M. E. (2019). Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. JAMA Network Open, 2(4), e192542. https://doi.org/10.1001/jamanetworkopen.2019.2542.

[4] Panfilova, E., & Knauss, E. (2021). Challenges and solutions when adopting DevSecOps: A systematic review. Information and Software Technology, 139, 106700. https://doi.org/10.1016/j.infsof.2021.106700

[5] Lee, A. R., Koo, D., Kim, I. K., Kim, H., & Park, J. (2023). Identifying facilitators of and barriers to the adoption of dynamic consent in digital health ecosystems: A scoping review. BMC Medical Ethics, 24, 107. https://doi.org/10.1186/s12910-023-00988-9

[6] Inkster B, Knibbs C, Bada M. Cybersecurity: a critical priority for digital mental health. Front Digit Health. 2023 Sep 14;5:1242264. doi: 10.3389/fdgth.2023.1242264. PMID: 37781452; PMCID: PMC10536959.

[7] Rindell, K., Ruohonen, J., Holvitie, J., Hyrynsalmi, S., & Leppänen, V. (2021). Security in agile software development: A practitioner survey. Information and Software Technology, 131, 106488. https://doi.org/10.1016/j.infsof.2020.106488.

[8] Wykes, T., Lipshitz, J. & Schueller, S.M. Towards the Design of Ethical Standards Related to Digital Mental Health and all Its Applications. Curr Treat Options Psych 6, 232–242 (2019). https://doi.org/10.1007/s40501-019-00180-0.

[9] Aljedaani B, Babar MA. Challenges With Developing Secure Mobile Health Applications: Systematic Review. JMIR Mhealth Uhealth. 2021 Jun 21;9(6):e15654. doi: 10.2196/15654. PMID: 34152277; PMCID: PMC8277314.

[10] Jawad, L. A. (2024). Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies. Abhigyan, 42(1), 23-31. https://doi.org/10.1177/09702385241233073 (Original work published 2024)

[11] Imran Mohammed, K., Shanmugam, B., & El-Den, J. (2025). Evolution of DevSecOps and its influence on application security: A systematic literature review. Technologies, 13(12), 548. https://doi.org/10.3390/technologies13120548.

[12] Firth, J., Torous, J., Nicholas, J., Carney, R., Pratap, A., Rosenbaum, S., & Sarris, J. (2017). The efficacy of smartphone-based mental health interventions for depressive symptoms: A meta-analysis of randomized controlled trials. World Psychiatry, 16(3), 287–298.https://doi.org/10.1002/wps.20472.

[13] Ienca M, Malgieri G. Mental data protection and the GDPR. J Law Biosci. 2022 Apr 25;9(1):lsac006. doi: 10.1093/jlb/lsac006. PMID: 35496983; PMCID: PMC9044203.

[14] Edo, O. C., Ang, D., Billakota, P., Salim, F. D., & Kanhere, S. S. (2024). A zero trust architecture for health information systems. Health and Technology, 14, 189–199. https://doi.org/10.1007/s12553-023-00809-4

[15] Ramaj, X., Sánchez-Gordón, M. L., Gkioulos, V., Chockalingam, S., & Colomo-Palacios, R. (2022). Holding on to compliance while adopting DevSecOps: A systematic literature review. Electronics, 11(22), 3707. https://doi.org/10.3390/electronics11223707.